

sense of the Senate that the Commander of Multinational Forces-Iraq and all United States personnel under his command should receive from Congress the full support necessary to carry out the United States mission in Iraq.

#### STATEMENTS ON INTRODUCED BILLS AND JOINT RESOLUTIONS

By Mr. LUGAR:

S. 494. A bill to endorse further enlargement of the North Atlantic Treaty Organization (NATO) and to facilitate the timely admission of new members to NATO, and for other purposes; to the Committee on Foreign Relations.

Mr. LUGAR. Mr. President, I rise today to introduce the "NATO Freedom Consolidation Act of 2007". Last year this legislation passed the Senate by unanimous consent. Unfortunately, the House was unable to act prior to adjournment last year.

I was pleased that thirteen of my colleagues, including Senators BIDEN, CHAMBLISS, COLEMAN, DODD, HAGEL, HUTCHISON, MARTINEZ, MCCAIN, SMITH, and SUNUNU, joined me in proposing this important legislation.

The goal of this bill is to reaffirm United States support for continued enlargement of NATO to democracies that are able and willing to meet the responsibilities of membership. In particular, the legislation calls for the timely admission of Albania, Croatia, Georgia, Macedonia, and Ukraine to NATO and authorizes security assistance for these countries in Fiscal Year 2008. Each of these countries has clearly stated its desire to join NATO and is working hard to meet the specified requirements for membership.

I believe that eventual NATO membership for these five countries would be a success for Europe, NATO, and the United States by continuing to extend the zone of peace and security. Albania, Croatia, and Macedonia have been making progress on reforms through their participation in the NATO Membership Action Plan since 2002. Unfortunately, Georgia and Ukraine have not yet been granted a Membership Action Plan but nevertheless have made remarkable progress. This legislation will provide important incentives and assistance to the countries to continue the implementation of democratic, defense, and economic reforms.

Since the end of the Cold War, NATO has been evolving to meet the new security needs of the 21st century. In this era, the threats to NATO members are transnational and far from its geographic borders. There is strong support among members for NATO's operation in Afghanistan, and for its training mission in Iraq. NATO's viability as an effective defense and security alliance depends on flexible, creative leadership, as well as the willingness of members to improve capabilities and address common threats.

If NATO is to continue to be the pre-eminent security Alliance and serve the defense interests of its membership, it must continue to evolve and that evolution must include enlargement. Potential NATO membership motivates emerging democracies to make important advances in areas such as the rule of law and civil society. A closer relationship with NATO will promote these values and contribute to our mutual security. Georgia is a young democracy that has made tremendous progress since the "Rose Revolution." It is situated in a critical geo-strategic location and is host to a large portion of the Baku-Tbilisi-Ceyhan pipeline that carries important energy resources to the West from Azerbaijan and, in the future, Kazakhstan. Georgia is resisting pressure from breakaway republics backed by Moscow. In the past, border disputes have been identified as reasons a country may not be invited to join NATO. But in this case, Russia's action, not Georgia's, are frustrating Tbilisi's NATO aspirations.

Three years ago, the United States Senate unanimously voted to invite seven countries to join NATO. Today, Bulgaria, Estonia, Latvia, Lithuania, Romania, Slovakia, and Slovenia are making significant contributions to NATO and are among our closest allies in the global war on terrorism. It is time again for the United States to take the lead in urging its allies to bring in new members, and to offer timely admission of Albania, Croatia, Georgia, Macedonia, and Ukraine to NATO.

By Mr. LEAHY (for himself, Mr. SPECTER, Mr. FEINGOLD, Mr. SCHUMER, and Mr. SANDERS):

S. 495. A bill to prevent and mitigate identity theft, to ensure privacy, to provide notice of security breaches, and to enhance criminal penalties, law enforcement assistance, and other protections against security breaches, fraudulent access, and misuse of personally identifiable information; to the Committee on the Judiciary.

Mr. LEAHY. Mr. President, today I am pleased to join Senator SPECTER in reintroducing the Leahy-Specter Personal Data Privacy and Security Act. This is a comprehensive data privacy package aimed at better protecting Americans' privacy. Senator SPECTER has been a valuable partner on this, and I also thank Majority Leader REID for his leadership and commitment to enacting data privacy legislation this year.

When Senator SPECTER and I introduced this bill in 2005, we had high hopes of bringing urgently needed data privacy reforms to the American people. The Judiciary Committee reported this bill favorably in November of 2005, but with the last Congress, it simply sat on the calendar. The leadership would not bring it forward.

The irony is while they refused to bring it forward, the problems of data

breaches remained a persistent and pernicious threat to Americans' privacy. Yesterday we learned that the Department of Veterans Affairs has lost a portable hard drive containing the sensitive personal information on as many as 48,000 veterans. I can imagine what the veterans in my State feel about that. I can imagine what the veterans in Montana feel about that.

Last week, there was a major data breach involving a State computer server in my home State of Vermont. It jeopardized the financial data of at least 69,000 Vermonters whose personal financial information had been stored on the computer used by the Vermont Agency of Human Services. Can you imagine 69,000 people, in a State of barely over 600,000 people.

This is not unique to Vermont. Last month mega retailer TJX disclosed that it suffered a major computer breach involving credit and debt card purchases involving possibly hundreds of thousands of American consumers. And, even as disturbing as that is, while they knew about the breach in mid-December, none of those customers were told about it until a month later. It is as if a thief had gone to each one of their houses and stolen their data.

Of course, all of this comes on the heels of the theft of the personal data of 26.5 million of our veterans and active-duty personnel at the VA last year. Think about this: You are a man or a woman serving your country in Afghanistan or Iraq, and this information is stolen—with data about where you live and what family members are left at home while you are overseas. How do you think that makes you feel?

According to the Privacy Rights Clearinghouse, more than 100 million records containing sensitive personal information have been involved in data security breaches since 2005. We need strong Federal data privacy and security laws to protect Americans' personal data, and to address the ills of lax data security.

Our bill requires that data brokers let consumers know what sensitive personal information they have about them and to allow individuals to correct this. It is a simple matter of fairness. There is a clear precedent for our approach in the credit reporting context. Our bill also requires that companies who have databases with sensitive personal information about Americans establish and implement data privacy and security programs. In the information age, any company that wants to be trusted by the public must earn that trust by vigilantly protecting the databases that they use and maintain. In addition, our bill requires notice when sensitive personal information has been compromised. The American people need to know when they may be exposed to a data breach. Whether it is a government agency or a private company, if they lose your sensitive information, your Social Security number, your address, or anything about you,

you have a right to know. If they are holding that information about you, and they lose it, you have the right to know it has been lost.

We also have tough criminal penalties for anyone who would intentionally or willfully conceal the fact that a data breach has occurred when that breach causes economic damage to consumers.

Then finally, we address the important issue of the Government's use of personal data. This would require Federal agencies to notify affected individuals when Government data breaches occur.

We should never have to worry about our Government having this information on us and losing it, but certainly in the last 2 or 3 years, we have seen so many millions of files that have been lost or put in jeopardy. We live in a world in which our Government also is increasingly turning to the private sector to get personal data that they, in some instances, couldn't legally get on their own. To address this, our bill puts protecting Americans' privacy first and foremost: Government data has to be protected and we have to know if the Government falls down on the job.

This is a comprehensive bill. It not only deals with the need to provide Americans notice when they have been victims of a data breach, it also deals with the underlying problems of lack of security and lack of accountability to prevent data breaches from occurring in the first place.

Today, Americans live in a world where their most sensitive personal information can be accessed and sold to the highest bidder with a few keystrokes on their computer. Our privacy laws greatly lag behind both the capabilities of our technology and the cunning of identity thieves. This legislation closes that gap. I commend the leadership for being willing to bring up our data privacy bill. I wish that the leadership in the last Congress had brought this bill up last year. But, I am glad that the new leadership will do so this year.

For the sake of all Americans, I urge all Senators to support this legislation and to act now to pass comprehensive data privacy and security legislation.

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

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

S. 495

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

#### SECTION 1. SHORT TITLE; TABLE OF CONTENTS.

(a) **SHORT TITLE.**—This Act may be cited as the "Personal Data Privacy and Security Act of 2007".

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

- Sec. 1. Short title; table of contents.
- Sec. 2. Findings.
- Sec. 3. Definitions.

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

- Sec. 101. Organized criminal activity in connection with unauthorized access to personally identifiable information.
- Sec. 102. Concealment of security breaches involving sensitive personally identifiable information.
- Sec. 103. Review and amendment of Federal sentencing guidelines related to fraudulent access to or misuse of digitized or electronic personally identifiable information.

#### TITLE II—DATA BROKERS

- Sec. 201. Transparency and accuracy of data collection.
- Sec. 202. Enforcement.
- Sec. 203. Relation to State laws.
- Sec. 204. Effective date.

#### TITLE III—PRIVACY AND SECURITY OF PERSONALLY IDENTIFIABLE INFORMATION

##### Subtitle A—A Data Privacy and Security Program

- Sec. 301. Purpose and applicability of data privacy and security program.
- Sec. 302. Requirements for a personal data privacy and security program.
- Sec. 303. Enforcement.
- Sec. 304. Relation to other laws.

##### Subtitle B—Security Breach Notification

- Sec. 311. Notice to individuals.
- Sec. 312. Exemptions.
- Sec. 313. Methods of notice.
- Sec. 314. Content of notification.
- Sec. 315. Coordination of notification with credit reporting agencies.
- Sec. 316. Notice to law enforcement.
- Sec. 317. Enforcement.
- Sec. 318. Enforcement by State attorneys general.
- Sec. 319. Effect on Federal and State law.
- Sec. 320. Authorization of appropriations.
- Sec. 321. Reporting on risk assessment exemptions.
- Sec. 322. Effective date.

##### TITLE IV—GOVERNMENT ACCESS TO AND USE OF COMMERCIAL DATA

- Sec. 401. General Services Administration review of contracts.
- Sec. 402. Requirement to audit information security practices of contractors and third party business entities.
- Sec. 403. Privacy impact assessment of government use of commercial information services containing personally identifiable information.
- Sec. 404. Implementation of chief privacy officer requirements.

#### SEC. 2. FINDINGS.

Congress finds that—

- (1) databases of personally identifiable information are increasingly prime targets of hackers, identity thieves, rogue employees, and other criminals, including organized and sophisticated criminal operations;
- (2) identity theft is a serious threat to the nation's economic stability, homeland security, the development of e-commerce, and the privacy rights of Americans;
- (3) over 9,300,000 individuals were victims of identity theft in America last year;
- (4) security breaches are a serious threat to consumer confidence, homeland security, e-commerce, and economic stability;
- (5) it is important for business entities that own, use, or license personally identifiable information to adopt reasonable procedures to ensure the security, privacy, and

confidentiality of that personally identifiable information;

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

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

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

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

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

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

#### SEC. 3. DEFINITIONS.

In this Act:

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

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

(3) **BUSINESS ENTITY.**—The term "business entity" means any organization, corporation, trust, partnership, sole proprietorship, unincorporated association, venture established to make a profit, or nonprofit, and any contractor, subcontractor, affiliate, or licensee thereof engaged in interstate commerce.

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

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

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

(7) **PERSONAL ELECTRONIC RECORD.**—

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

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

- (i) any data related to an individual's past purchases of consumer goods; or
- (ii) any proprietary assessment or evaluation of an individual or any proprietary assessment or evaluation of information about an individual.

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

(9) **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.

(10) **SECURITY BREACH.**—

(A) **IN GENERAL.**—The term “security breach” means compromise of the security, confidentiality, or integrity of computerized data through misrepresentation or actions that result in, or there is a reasonable basis to conclude has resulted in, acquisition of or access to sensitive personally identifiable information that is unauthorized or in excess of authorization.

(B) **EXCLUSION.**—The term “security breach” does not include—

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

(ii) the release of a public record, or information derived from a single public record, not otherwise subject to confidentiality or nondisclosure requirement, or information obtained from a news report or periodical.

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

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

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

(ii) Any 2 of the following:

(I) Home address or telephone number.

(II) Mother’s maiden name, if identified as such.

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

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

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

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

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

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

Section 1961(1) of title 18, United States Code, is amended by inserting “section 1030(a)(2)(D) (relating to fraud and related activity in connection with unauthorized access to sensitive personally identifiable information as defined in the Personal Data Privacy and Security Act of 2007,” before “section 1084”.

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

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

#### **“§ 1040. Concealment of security breaches involving sensitive personally identifiable information**

“(a) Whoever, having knowledge of a security breach and of the obligation to provide notice of such breach to individuals under title III of the Personal Data Privacy and Security Act of 2007, and having not otherwise qualified for an exemption from providing notice under section 312 of such Act, intentionally and willfully conceals the fact of such security breach and which breach causes economic damage to 1 or more persons, shall be fined under this title or imprisoned not more than 5 years, or both.

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

“(c) Any person seeking an exemption under section 312(b) of the Personal Data Privacy and Security Act of 2007 shall be immune from prosecution under this section if the United States Secret Service does not indicate, in writing, that such notice be given under section 312(b)(3) of such Act”.

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

“1040. Concealment of security breaches involving personally identifiable information.”

(c) **ENFORCEMENT AUTHORITY.**—

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

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

### **SEC. 103. REVIEW AND AMENDMENT OF FEDERAL SENTENCING GUIDELINES RELATED TO FRAUDULENT ACCESS TO OR MISUSE OF DIGITIZED OR ELECTRONIC PERSONALLY IDENTIFIABLE INFORMATION.**

(a) **REVIEW AND AMENDMENT.**—The United States Sentencing Commission, pursuant to its authority under section 994 of title 28, United States Code, and in accordance with this section, shall review and, if appropriate, amend the Federal sentencing guidelines (including its policy statements) applicable to persons convicted of using fraud to access, or misuse of, digitized or electronic personally identifiable information, including identity theft or any offense under—

(1) sections 1028, 1028A, 1030, 1030A, 2511, and 2701 of title 18, United States Code; and

(2) any other relevant provision.

(b) **REQUIREMENTS.**—In carrying out the requirements of this section, the United States Sentencing Commission shall—

(1) ensure that the Federal sentencing guidelines (including its policy statements) reflect—

(A) the serious nature of the offenses and penalties referred to in this Act;

(B) the growing incidences of theft and misuse of digitized or electronic personally identifiable information, including identity theft; and

(C) the need to deter, prevent, and punish such offenses;

(2) consider the extent to which the Federal sentencing guidelines (including its policy statements) adequately address violations of the sections amended by this Act to—

(A) sufficiently deter and punish such offenses; and

(B) adequately reflect the enhanced penalties established under this Act;

(3) maintain reasonable consistency with other relevant directives and sentencing guidelines;

(4) account for any additional aggravating or mitigating circumstances that might justify exceptions to the generally applicable sentencing ranges;

(5) consider whether to provide a sentencing enhancement for those convicted of the offenses described in subsection (a), if the conduct involves—

(A) the online sale of fraudulently obtained or stolen personally identifiable information;

(B) the sale of fraudulently obtained or stolen personally identifiable information to an individual who is engaged in terrorist activity or aiding other individuals engaged in terrorist activity; or

(C) the sale of fraudulently obtained or stolen personally identifiable information to finance terrorist activity or other criminal activities;

(6) make any necessary conforming changes to the Federal sentencing guidelines to ensure that such guidelines (including its policy statements) as described in subsection (a) are sufficiently stringent to deter, and adequately reflect crimes related to fraudulent access to, or misuse of, personally identifiable information; and

(7) ensure that the Federal sentencing guidelines adequately meet the purposes of sentencing under section 3553(a)(2) of title 18, United States Code.

(c) **EMERGENCY AUTHORITY TO SENTENCING COMMISSION.**—The United States Sentencing Commission may, as soon as practicable, promulgate amendments under this section in accordance with procedures established in section 21(a) of the Sentencing Act of 1987 (28 U.S.C. 994 note) as though the authority under that Act had not expired.

## **TITLE II—DATA BROKERS**

### **SEC. 201. TRANSPARENCY AND ACCURACY OF DATA COLLECTION.**

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

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

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

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

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

(4) information in a personal electronic record that—

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

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

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

(C) DISCLOSURES TO INDIVIDUALS.—

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

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

(D) ACCURACY RESOLUTION PROCESS.—

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

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

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

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

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

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

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

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

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

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

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

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

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

**SEC. 202. ENFORCEMENT.**

(a) CIVIL PENALTIES.—

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

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

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

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

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

(c) STATE ENFORCEMENT.—

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

(A) enjoin that act or practice;

(B) enforce compliance with this title; or

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

(2) NOTICE.—

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

(i) a written notice of that action; and

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

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

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

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

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

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

(C) file petitions for appeal.

(4) PENDING PROCEEDINGS.—If the Federal Trade Commission has instituted a pro-

ceeding or civil action for a violation of this title, no attorney general of a State may, during the pendency of such proceeding or civil action, bring an action under this subsection against any defendant named in such civil action for any violation that is alleged in that civil action.

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

(A) conduct investigations;

(B) administer oaths and affirmations; or

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

(6) VENUE; SERVICE OF PROCESS.—

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

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

(i) is an inhabitant; or

(ii) may be found.

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

**SEC. 203. RELATION TO STATE LAWS.**

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

**SEC. 204. EFFECTIVE DATE.**

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

**TITLE III—PRIVACY AND SECURITY OF PERSONALLY IDENTIFIABLE INFORMATION**

**Subtitle A—A Data Privacy and Security Program**

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

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

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

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

(1) FINANCIAL INSTITUTIONS.—Financial institutions—

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

(B) subject to—

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

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

(2) HIPPA REGULATED ENTITIES.—

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

(B) BUSINESS ENTITIES.—A business entity shall be deemed in compliance with the privacy and security program requirements under section 302 if the business entity is acting as a “business associate” as that term is defined in the Health Insurance Portability and Accountability Act of 1996 (42 U.S.C. 1301 et seq.) and is in compliance with requirements imposed under that Act and its implementing regulations.

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

(d) SAFE HARBORS.—

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

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

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

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

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

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

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

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

(C) protect against unauthorized access to use of sensitive personally identifying information that could result in substantial harm or inconvenience to any individual.

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

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

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

(C) assess the sufficiency of its policies, technologies, and safeguards in place to control and minimize risks from unauthorized

access, disclosure, use, or alteration of sensitive personally identifiable information; and

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

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

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

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

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

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

(iii) protect sensitive personally identifiable information during use, transmission, storage, and disposal by encryption 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); and

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

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

(c) VULNERABILITY TESTING.—

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

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

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

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

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

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

(1) technology;

(2) the sensitivity of personally identifiable information;

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

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

(A) mergers and acquisitions;

(B) alliances and joint ventures;

(C) outsourcing arrangements;

(D) bankruptcy; and

(E) changes to sensitive personally identifiable information systems.

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

#### SEC. 303. ENFORCEMENT.

(a) CIVIL PENALTIES.—

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

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

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

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

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

(c) STATE ENFORCEMENT.—

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

(A) enjoin that act or practice;

(B) enforce compliance with this subtitle; or

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

(2) NOTICE.—

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

(i) a written notice of that action; and

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

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

(C) NOTIFICATION WHEN PRACTICABLE.—In an action described under subparagraph (B), the attorney general of a State shall provide the

written notice and the copy of the complaint to the Federal Trade Commission as soon after the filing of the complaint as practicable.

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

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

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

(C) file petitions for appeal.

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

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

(A) conduct investigations;

(B) administer oaths and affirmations; or

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

(6) **VENUE; SERVICE OF PROCESS.**—

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

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

(i) is an inhabitant; or

(ii) may be found.

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

#### **SEC. 304. RELATION TO OTHER LAWS.**

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

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

#### **Subtitle B—Security Breach Notification**

##### **SEC. 311. NOTICE TO INDIVIDUALS.**

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

(b) **OBLIGATION OF OWNER OR LICENSEE.**—

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

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

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

(c) **TIMELINESS OF NOTIFICATION.**—

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

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

(3) **BURDEN OF PROOF.**—The agency, business entity, owner, or licensee required to provide notification under this section shall have the burden of demonstrating that all notifications were made as required under this subtitle, including evidence demonstrating the reasons for any delay.

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

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

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

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

##### **SEC. 312. EXEMPTIONS.**

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

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

(A) cause damage to the national security; or

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

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

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

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

(C) restrain competition.

(3) **NOTICE.**—In every case in which an agency issues a certification under paragraph (1), the certification, accompanied by a description of the factual basis for the cer-

tification, shall be immediately provided to the United States Secret Service.

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

(1) a risk assessment concludes that there is no significant risk that the security breach has resulted in, or will result in, harm to the individuals whose sensitive personally identifiable information was subject to the security breach;

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

(A) the results of the risk assessment; and

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

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

(c) **FINANCIAL FRAUD PREVENTION EXEMPTION.**—

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

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

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

(2) **LIMITATION.**—The exemption by this subsection does not apply if the information subject to the security breach includes sensitive personally identifiable information in addition to the sensitive personally identifiable information identified in section 3.

##### **SEC. 313. METHODS OF NOTICE.**

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

(1) **INDIVIDUAL NOTICE.**—

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

(B) Telephone notice to the individual personally; or

(C) Electronic notice, if the primary method used by the agency or business entity to communicate with the individual is by electronic means, or the individual has consented to receive such notice and the notice is consistent with the provisions permitting electronic transmission of notices under section 101 of the Electronic Signatures in Global and National Commerce Act (15 U.S.C. 7001).

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

##### **SEC. 314. CONTENT OF NOTIFICATION.**

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

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

(2) a toll-free number or, if the primary method used by the agency or business entity to communicate with the individual is by electronic means, an electronic mail address—

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



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

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

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

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

If an agency or business entity is required to provide notification to more than 1,000 individuals under section 311(a), the agency or business entity shall also notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis (as defined in section 603(p) of the Fair Credit Reporting Act (15 U.S.C. 1681a(p)) of the timing and distribution of the notices.

**SEC. 316. NOTICE TO LAW ENFORCEMENT.**

(a) **SECRET SERVICE.**—Any business entity or agency shall give notice of a security breach to the United States Secret Service if—

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

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

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

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

(b) **NOTICE TO OTHER LAW ENFORCEMENT AGENCIES.**—The United States Secret Service shall be responsible for notifying—

(1) the Federal Bureau of Investigation, if the security breach involves espionage, foreign counterintelligence, information protected against unauthorized disclosure for reasons of national defense or foreign relations, or Restricted Data (as that term is defined in section 11y of the Atomic Energy Act of 1954 (42 U.S.C. 2014(y))), except for offenses affecting the duties of the United States Secret Service under section 3056(a) of title 18, United States Code;

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

(3) the attorney general of each State affected by the security breach.

(c) **14-DAY RULE.**—The notices to Federal law enforcement and the attorney general of each State affected by a security breach required under this section shall be delivered as promptly as possible, but not later than 14 days after discovery of the events requiring notice.

**SEC. 317. ENFORCEMENT.**

(a) **CIVIL ACTIONS BY THE ATTORNEY GENERAL.**—The Attorney General may bring a civil action in the appropriate United States district court against any business entity that engages in conduct constituting a violation of this subtitle and, upon proof of such conduct by a preponderance of the evidence, such business entity shall be subject to a civil penalty of not more than \$1,000 per day per individual whose sensitive personally identifiable information was, or is reasonably believed to have been, accessed or ac-

quired by an unauthorized person, up to a maximum of \$1,000,000 per violation, unless such conduct is found to be willful or intentional.

(b) **INJUNCTIVE ACTIONS BY THE ATTORNEY GENERAL.**—

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

(A) enjoining such act or practice; or

(B) enforcing compliance with this subtitle.

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

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

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

**SEC. 318. ENFORCEMENT BY STATE ATTORNEYS GENERAL.**

(a) **IN GENERAL.**—

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

(A) enjoin that practice;

(B) enforce compliance with this subtitle; or

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

(2) **NOTICE.**—

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

(i) written notice of the action; and

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

(B) **EXEMPTION.**—

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

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

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

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

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

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

(4) file petitions for appeal.

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

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

(1) conduct investigations;

(2) administer oaths or affirmations; or

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

(e) **VENUE; SERVICE OF PROCESS.**—

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

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

(B) another court of competent jurisdiction.

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

(A) is an inhabitant; or

(B) may be found.

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

**SEC. 319. EFFECT ON FEDERAL AND STATE LAW.**

The provisions of this subtitle shall supersede any other provision of Federal law or any provision of law of any State relating to notification of a security breach, except as provided in section 314(b).

**SEC. 320. AUTHORIZATION OF APPROPRIATIONS.**

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

**SEC. 321. REPORTING ON RISK ASSESSMENT EXEMPTIONS.**

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

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

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

**SEC. 322. EFFECTIVE DATE.**

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

# **TITLE IV—GOVERNMENT ACCESS TO AND USE OF COMMERCIAL DATA**

## **SEC. 401. GENERAL SERVICES ADMINISTRATION REVIEW OF CONTRACTS.**

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

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

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

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

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

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

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

(1) include monetary or other penalties—

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

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

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

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

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

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

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

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

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

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

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

(3) by adding at the end the following:

“(9) procedures for evaluating and auditing the information security practices of con-

tractors or third party business entities supporting the information systems or operations of the agency involving personally identifiable information (as that term is defined in section 3 of the Personal Data Privacy and Security Act of 2007) and ensuring remedial action to address any significant deficiencies.”.

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

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

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

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

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

“(iii) purchasing or subscribing for a fee to personally identifiable information from a data broker (as such terms are defined in section 3 of the Personal Data Privacy and Security Act of 2007).”.

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

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

(A) such database;

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

(C) the amount of the contract for use;

(2) adopts regulations that specify—

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

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

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

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

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

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

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

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

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

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

(A) providing for penalties—

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

(ii) if the entity knows or has reason to know that the personally identifiable infor-

mation being provided to the Federal department or agency is inaccurate, and provides such inaccurate information; and

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

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

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

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

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

(d) STUDY OF GOVERNMENT USE.—

(1) SCOPE OF STUDY.—Not later than 180 days after the date of enactment of this Act, the Comptroller General of the United States shall conduct a study and audit and prepare a report on Federal agency use of data brokers or commercial databases containing personally identifiable information, including the impact on privacy and security, and the extent to which Federal contracts include sufficient provisions to ensure privacy and security protections, and penalties for failures in privacy and security practices.

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

## **SEC. 404. IMPLEMENTATION OF CHIEF PRIVACY OFFICER REQUIREMENTS.**

(a) DESIGNATION OF THE CHIEF PRIVACY OFFICER.—Pursuant to the requirements under section 522 of the Transportation, Treasury, Independent Agencies, and General Government Appropriations Act, 2005 (division H of Public Law 108-447; 118 Stat. 3199) that each agency designate a Chief Privacy Officer, the Department of Justice shall implement such requirements by designating a department-wide Chief Privacy Officer, whose primary role shall be to fulfill the duties and responsibilities of Chief Privacy Officer and who shall report directly to the Deputy Attorney General.

(b) DUTIES AND RESPONSIBILITIES OF CHIEF PRIVACY OFFICER.—In addition to the duties and responsibilities outlined under section 522 of the Transportation, Treasury, Independent Agencies, and General Government Appropriations Act, 2005 (division H of Public Law 108-447; 118 Stat. 3199), the Department of Justice Chief Privacy Officer shall—

(1) oversee the Department of Justice's implementation of the requirements under section 403 to conduct privacy impact assessments of the use of commercial data containing personally identifiable information by the Department; and

(2) coordinate with the Privacy and Civil Liberties Oversight Board, established in the Intelligence Reform and Terrorism Prevention Act of 2004 (Public Law 108-458), in implementing this section.

Mr. SPECTER. Mr. President, I seek recognition today to discuss the Personal Data Privacy and Security Act of 2007, which I am introducing with Senator LEAHY. Not long ago, personal information—Social Security numbers, birthdates, mothers' maiden names, addresses—all remained relatively private. Some information—for example,



whether you had a mortgage on your home—might have been publicly available, but finding that information required a trip to the local courthouse. For the most part, the sheer difficulty of obtaining personal information kept it private. This privacy—what Justice Brandeis called the freedom to be left alone—has been a cherished value throughout American history.

As everyday transactions increasingly occur electronically, personal information can be stored, transmitted and accessed much more easily. Most Americans have benefited from this change. Because personal information is available electronically, Americans enjoy the convenience of purchasing goods over the phone or on the Internet. They can obtain a home mortgage in a matter of hours. They can apply for a credit card while they wait at the store. The availability of such information also helps law enforcement agencies conduct investigations and apprehend criminals.

In electronic form, personal information is both more valuable and more vulnerable. As the multitude of security breaches that have occurred over the past 2 years demonstrate, electronic information is more vulnerable because it can be accessed anonymously from afar and can be stolen in a split second. According to the Privacy Rights Clearing House, since February 2005, over 100 million records containing personal information have been subject to some sort of security breach. The first of these incidents to come to light involved commercial data broker ChoicePoint, which in February 2005 reported that identity thieves had gained access to personal information of 163,000 people. The identity thieves had obtained the information by setting up sham accounts with ChoicePoint. ChoicePoint eventually settled with the FTC for \$15 million, including \$5 million for consumer redress. However, consumers might never have found out about the breach. The incident only came to light because of a law California had recently adopted requiring ChoicePoint and others to provide notice of security breaches involving personal information to California residents who were affected by the breach. As a result of the California law, Americans for the first time began learning that data brokers and others were routinely collecting and selling their personal information, and in so doing, they were not always keeping the information secure.

After the ChoicePoint incident came a long series of security breaches involving major American companies. In March of 2005, Designer Shoe Warehouse reported that hackers had gained access to personal information, including credit card numbers, on over 100,000 of its customers. Weeks later, Lexis Nexis reported that hackers had gained access to the personal information of over 300,000 individuals. Other blue-chip companies where unauthorized persons have gained access to personal

information include Wal-Mart, General Motors, Wachovia Bank, H&R Block, Honeywell, AT&T, Lloyd's of London, ARCO, Visa, MasterCard, Bank of America, FedEx, OfficeMax, Blue Cross Blue Shield and Ralph Lauren. The largest incident came in June 2005, when Card Systems, which processes payments for the country's largest banks and credit card companies, reported that hackers had accessed 40 million records containing personal information. Most recently, TJ Maxx Stores and MoneyGram both had the personal information of their customers stolen from their computer systems. This list only includes security breaches involving wrong-doers who were trying to obtain personal information. The list would be much longer had it included inadvertent disclosure of personal information or incidents involving stolen computers or other equipment that happened to contain personal information.

A large number of colleges and universities have also suffered significant breaches, including the University of Southern California, which in July of 2005 reported that hackers has accessed 270,000 records containing personal data. Other educational institutions that have been hacked include Boston College, Northwestern University, Tufts University, UCLA, Michigan State, Carnegie Mellon, Purdue, Stanford, Duke, the University of Iowa, the University of Colorado, and the University of Utah.

Governments also have not been immune from attempts by identity thieves to obtain personal information. Hackers have accessed personal data at the Department of Defense, Department of Energy, the Air Force and the Department of Agriculture. Hackers obtained over half a million records containing personal data from a State agency in Georgia. The San Diego County Employees Retirement Association, the California Department of Corrections, the Nebraska Treasurers office, the city of Lubbock, TX, and a Women, Infants and Children (WIC) program in Hawaii have all been the victims of similar thefts.

Electronic personal data is more valuable because identity thieves can steal a large volume of data and use it before anyone even knows their personal information has been compromised. For the last 5 years, identity theft has topped the FTC's list of consumer complaints. From 2002 to 2004, the number of complaints rose 52 percent, to 246,570. Put another way, that's one complaint every 2 minutes. But this is only the tip of the iceberg. Not all consumers report identity theft to the FTC. Not all victims report identity theft to their local police. Sixty percent of those who did file a report with the FTC did not call their local police department. It stands to reason that many did not call the FTC.

A recent study by the Better Business Bureau concluded that 8.9 million Americans were victims of identity

fraud in 2006, and that each victim lost approximately \$6,300. Ultimately, it has been predicted that nearly 20 percent of Americans will become victims of identity theft. Worse, according to the study, it took victims an average of 40 hours on the phone with creditors and credit bureaus to clear their names. I use the term "clear" loosely, because in many cases the damage caused by identity theft is irreversible. Victims will have fraud alerts on their credit reports for years to come, making it more difficult for them to open new accounts or make major purchases. Some will be erroneously contacted by collection agencies. Many will not even know they have been victimized until they try to get a car loan or a mortgage on a home.

Individuals who have not yet been victims also suffer. Businesses lose nearly \$50 billion a year from identity thieves posing as customers. These losses translate into increased prices for every consumer. All Americans are victims of identity theft, even if their own information remains secure.

In some cases, the availability of electronic personal data can lead to tragedy. In 1999, a former high school classmate of Amy Lynn Boyer obtained her former work address and Social Security number from an on-line data broker. Using this information, he called Amy's mother and posed as the former employer, convincing Amy's mom to give him Amy's new work address. He then drove to Amy's workplace and fatally shot her.

In an effort to protect the privacy and security of our personal information, and prevent future tragedies, small and large, last Congress, Senator LEAHY and I introduced the Personal Data Privacy and Security Act. The problem is one of large proportions and many have views on how to go about tackling it. Six committees, three on the House side and three on the Senate side, introduced legislation last Congress addressing data security. At least two other Senate committees became involved in the issue. It is my hope that the differences among committees and members can be bridged this Congress. The problem is simply too large to ignore.

In an effort to start that process, Senator LEAHY and I are again introducing the Personal Data Privacy and Security Act. We are reintroducing the bill in largely the same form that it was approved by the Judiciary Committee last Congress. The bill takes a comprehensive approach to the problem, an approach I believe is necessary. First, the legislation goes after identity thieves by increasing penalties for crimes involving electronic personal information. It also contains criminal penalties for those who intentionally conceal a security breach involving personal data. Those who actively conceal breaches attempt to protect themselves by gambling with the reputations and finances of innocent Americans. They deserve to be punished.

The bill also empowers Americans to look after the privacy of their own information. The bill will allow individuals to gain access to their personal information when it is in the hands of commercial data brokers. For individuals who believe their information is wrong—possibly because the activities of identity thieves—data brokers must provide assistance with correcting their information.

The legislation also places some of the burden of protecting privacy on those that collect personal information. It will require the companies, government agencies, universities and others that deal with personal information to identify and remedy any weaknesses in their computer systems.

Such measures will not always be enough. As I've already noted, the nature of electronic information makes it vulnerable even when reasonable steps are taken to protect it. Currently, over 30 States have adopted legislation requiring companies, agencies, universities and others to give notice when they experience a security breach that involves personal information. However, no Federal law imposes such a requirement. As a result, companies are forced to comply with over 30 different State laws, an expensive and time-consuming endeavor.

The Personal Data Privacy and Security Act requires that both affected individuals and law enforcement receive notice. Knowledge is power. Once individuals learn that their personal information is exposed, they can take steps to protect themselves. And, the company, school or agency that experienced the breach must help. They must provide individuals whose data was lost with credit monitoring. For large breaches, the media must be notified. Media reports over the 2 years have made Americans far more aware of the problem of security breaches. Hopefully, we can raise awareness by continuing the practice of making public announcements. Notice will also give law enforcement a head start in catching those who steal personal information.

Finally, this legislation will protect the privacy of all Americans by providing a check on the government's use of commercial databases. Federal law enforcement agencies use commercial databases to track criminals and criminal activity. Correctly used, these databases can be very useful tools in the fight against crime. However, there should be some check on their use. The bill makes it clear that protections similar to those provided by the Privacy Act are applied to the government's use of commercial databases. The legislation also aims at making sure the government's use of such data is secure.

This bill represents a comprehensive effort to protect the privacy and security of the personal information of all Americans. The lives of most Americans have been made easier because our personal information is readily avail-

able to those who have a legitimate need for it. This legislation aims to keep such information out of the hands of those who have no legitimate need for it. I want to take a moment to thank my colleague, Senator LEAHY, who has been tireless in his efforts to promote individual privacy. He has long fought these issues on the Senate floor and has been a leader in securing the privacy rights of all Americans. I urge my colleagues to join us in supporting this important legislation.

Mr. FEINGOLD. Mr. President, I am proud to be an original cosponsor of the Personal Data Privacy and Security Act of 2007. This bill is a much-needed solution to the daunting problem of ensuring the privacy and the security of our personal data, which has become such a precious commodity.

Several forces are converging to make our personal information more valuable—and more vulnerable—than ever. The world is digital and so is our personal data. In this day and age, almost everything we do results in a third party creating a digital record about us—digital records that we may not even realize exist. We seek the convenience of opening bank accounts, managing our credit cards, and making major purchases over the Internet. And we often complete these transactions without ever speaking to another person face-to-face or over the telephone. Businesses, nonprofits, and political parties are personalizing their messages, products, and services to a degree we've never seen before, and they are willing to invest significant amounts of money in collecting personal information about potential customers or donors. And we are living in an age where identity-based screening and security programs can be vitally important, resulting in more information being collected about individuals in an attempt to identify them accurately.

As a result, personal information has become a hot commodity that is bought, sold, and—as so often happens when something becomes valuable—stolen.

We are at a crossroads. We all know about the security breaches that have been on the front pages of newspapers. They have placed the identities of hundreds of thousands of Americans at risk. The fear among the American public is so widespread that it has become the basis of an entire ad campaign by a credit card company.

But this is about much more than information security. Until California law required a company named ChoicePoint to notify individuals in 2005 that their information was compromised and that they might be vulnerable to identity theft, many Americans had never heard of ChoicePoint. As news stories focused on the data broker business, many Americans were surprised to discover that companies are creating digital dossiers about them that contain massive amounts of information, and that these companies

sell that information to commercial and government entities. The revelations about these security breaches highlighted the fact that Americans need a better understanding of what happens to their information in a digital world—and what kind of consequences they can face as a result.

When I am back home in Wisconsin, I hear from people who do not understand why companies have the right to sell their sensitive personal information. I hear from people who are shocked to discover that personal information about them is available for free on the Internet.

There is no question that data aggregators facilitate societal benefits, allowing consumers to obtain instant credit and personalized services, and allowing police officers to locate suspects. But these companies also gather a great deal of potentially sensitive information about individuals, and in many instances they go largely unregulated.

Too many of my constituents feel that they have lost control over their own information. Congress must return some power to individual Americans so that we can all better understand and manage what happens to our own personal data.

The Personal Data Privacy and Security Act takes a comprehensive approach to the privacy and security problems we face. It gives consumers back some control over their own information. The bill requires data brokers to allow consumers to access their own information and to investigate when consumers tell them that corrections are necessary. And it requires companies to give notice to affected consumers and to law enforcement if there is a serious security breach, so that individuals know their identity may be at risk and can take steps to protect themselves.

In addition, the bill extends existing criminal law to ensure that it covers unauthorized access of data broker systems, as well as concealment of security breaches. It requires companies that buy and sell information to have appropriate data security systems in place. These protections will help safeguard against future privacy violations and security breaches in the commercial data industry. But that is not all this bill accomplishes.

The bill also contains some critically important privacy and security provisions to govern the government's use of commercial data. This is an aspect of the data broker business that has not yet gotten as much attention in the wake of the security breaches over the past few years. The information gathered by these companies is not just sold to individuals and businesses; government agencies of all stripes also buy or subscribe to information from commercial sources. We all remember the discovery in 2005 that the Pentagon had a contract with a marketing firm to analyze commercial and other data about high school and college students.

Although the government should be able to access commercial databases in appropriate circumstances, there are few existing rules or guidelines to ensure this information is used responsibly. Nor are there restrictions on the use of commercial data for powerful, intrusive data mining programs. The Privacy Act, which governs when government agencies themselves are collecting data, likely does not apply because the information is held outside the government and is not gathered solely at government direction.

As a result, there is a great deal we do not know about government use of commercial data, even in clearly appropriate circumstances such as when the agency's goal is simply to locate an individual already suspected of a crime.

We don't know under what circumstances government employees can obtain access to these databases or for what purposes. We don't know how government agencies evaluate the accuracy of the databases to which they subscribe. We don't know how the accuracy level of the data affects government use of the data. We don't know how employees are monitored to ensure they do not abuse their access to these databases. We don't know how those who misuse the information are punished. And we don't know how government agencies, particularly those engaged in sensitive national security investigations, ensure that the data brokers cannot keep records of who the government is investigating, records which themselves could create a huge security risk in light of the vulnerabilities that have come to the forefront in recent months.

That is why I am so pleased that this bill includes provisions to address the government's use of commercial data. A comprehensive approach to data privacy and security would be incomplete without taking on this piece of the puzzle. The bill recognizes there are many legitimate reasons for government agencies to obtain commercially available data, but that they need to be subject to privacy and security protections. It takes a common sense approach, pushing government agencies to take basic steps to ensure that individuals' personal information is secure and only used for legitimate purposes, and that the commercial information the government is paying for and relying on is accurate and complete.

Specifically, the bill would require that federal agencies that subscribe to commercial data adopt standards governing its use. These standards would reflect long-standing basic privacy principles. The bill would ensure that government agencies consider and determine which personnel will be permitted to access the information and under what circumstances; develop retention policies for this personal data and get rid of data they no longer need, minimizing the opportunity for abuse or theft; rely only on accurate and complete data, and penalize vendors

who knowingly provide inaccurate information to the Federal Government; provide individuals who suffer adverse consequences as a result of the agency's reliance on commercial data with a redress mechanism; and establish enforcement mechanisms for those privacy policies.

The bill also directs the General Services Administration to review government contracts for commercial data to make sure that vendors have appropriate security programs in place, and that they do not provide information to the government that they know to be inaccurate. And it requires agencies to audit the information security practices of their vendors.

These are basic good government measures. They guarantee that the Federal Government is not wasting money on inaccurate data and that vendors are undertaking the security programs that they have promised and for which the government is paying.

We live in a new digital world. The law may never fully keep up with technology, but we must make every effort we can. I am proud to be involved in this comprehensive, reasoned approach to privacy and security, and I hope it will move forward in this Congress. I congratulate Senators LEAHY and SPECTER for their excellent work on this bill. This bill is important and it deserves serious consideration.

By Mrs. BOXER:

S. 497. A bill to repeal a prohibition on the use of certain funds for tunneling in certain areas with respect to the Los Angeles to San Fernando Valley Metro Rail project, California; to the Committee on Banking, Housing, and Urban Affairs.

Mrs. BOXER. Mr. President, today I rise to introduce a bill for myself and Senator FEINSTEIN to allow for subway tunneling in parts of Los Angeles.

In 1985, in response to a methane gas explosion that destroyed a Ross Dress for Less Store in Los Angeles, Representative WAXMAN worked to enact a law that prohibits subway tunneling in his district.

In 2004, the Los Angeles City Council passed a motion in support of reversing the laws banning tunneling. In February 2005, the Los Angeles Metropolitan Transportation Authority board also voted to begin discussions of subway expansion.

As a result, a panel of scientific experts was created to conduct an independent safety review that determined that subway tunneling could move forward safely with new technology.

Representative WAXMAN introduced a bill to lift the Federal tunneling prohibition in the last Congress—where it passed the House—and again in this Congress. Senator FEINSTEIN and I are introducing the same bill in the Senate.

This legislation has the support of Los Angeles Mayor Antonio Villaraigosa and the Los Angeles Metropolitan Transportation Authority.

This bill is necessary to expand the subway, which is extremely important in Los Angeles—a city that ranks time and time again as the most congested region in the country. The Wilshire corridor is densely populated and is a large commercial area. The freeways and streets are filled—we need transit in this area.

By Mr. FEINGOLD (for himself and Ms. COLLINS):

S. 498. A bill to amend title XVIII of the Social Security Act to improve the Medicare program for beneficiaries residing in rural areas; to the Committee on Finance.

Mr. FEINGOLD. Mr. President, today, along with my colleague Senator COLLINS from Maine, I am introducing legislation to address the needs of the nearly one-quarter of all Medicare beneficiaries who live in rural America. These beneficiaries are systematically disadvantaged in the Medicare program. The beauty of Medicare is its equity, its universality, and its accessibility. But we have compromised these values by stratifying payments, by under-representing rural voices on the Medicare Payment Advisory Commission, and by continuing to use obsolete payment data that hurts rural America.

First, we must stop indexing physician payments for work based on geographic differences. Rural areas already have a hard enough time recruiting and retaining the Nation's top talent. Currently, even though 25 percent of Medicare beneficiaries live in rural areas, only 10 percent of the Nation's physicians serve them. Lower payments to doctors in these areas only perpetuate this dangerous shortage of medical expertise. We should not be discouraging medical school graduates from moving to underserved rural areas by continuing to offer sub-par pay—in fact, we should be providing incentives to encourage them to work in underserved areas. My legislation proposes a project to help rural facilities to host educators and clinical practitioners in clinical rotations.

Lack of dollars to rural health facilities has also prevented communities from investing in vital information technology. The Institute of Medicine published a report in 2005 detailing the ways in which health IT could assist isolated communities. For example, since rural physicians tend to be generalists rather than specialists, virtual libraries within physician offices would provide both doctors and patients with a wider and deeper source of information at their fingertips. Rural residents can also be quite far from health facilities, so technology that allows emergency room physicians to communicate with EMS workers in an ambulance can help patients receive life-saving treatment before they physically reach the hospital. These kinds of technologies will improve both the quality and efficiency of care given in rural areas. My legislation offers funding for

quality improvement demonstration projects, to allow isolated communities to invest in this otherwise out of reach technology.

Lastly, this legislation will end the disproportionately low representation of rural interests on the Medicare Payment Advisory Commission. This lack of representation has resulted in policies that hurt rural communities. Those policies have hurt—and continue to hurt—the people of my State of Wisconsin, and they hurt my colleague Senator COLLINS' constituents as well. For every dollar that Medicare spends on the average beneficiary in the average State in this country, Medicare spends only 82 cents on a beneficiary in Wisconsin. In Maine, Medicare spends only 80 cents per dollar it spends on the average beneficiary.

How is this the case, if beneficiaries in Wisconsin and in Maine pay the same payroll taxes as beneficiaries in other States? Because the distribution of Medicare dollars among the 50 States is grossly unfair to Wisconsin, and to much of the Upper Midwest. Wisconsinites pay payroll taxes just like every American taxpayer, but the Medicare funds we get in return are lower than those received in many other States.

With the guidance and support of people across my State who are fighting for Medicare fairness, I am introducing this legislation to address Medicare's discrimination against Wisconsin's seniors and health care providers. My bill will decrease some of the inequitable payments that harm rural areas. It will provide rural areas the help they need to grow crucial health information technology infrastructure. It will offer the necessary incentives to help attract the Nation's top medical talent to underserved rural areas. And it will mandate rural representation on the Medicare Payment Advisory Commission. Rural seniors are already underserved in their communities; they should not be underrepresented in Washington as well.

Rural Americans have worked hard and paid into the Medicare program all their lives. In return, they deserve full access to the same benefits as seniors throughout the country: their choice of highly skilled physicians, use of the latest technologies, and a strong voice representing their needs in Medicare policy.

I ask unanimous consent that the text of my bill be printed in the RECORD.

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

S. 498

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

#### SECTION 1. SHORT TITLE; TABLE OF CONTENTS.

(a) SHORT TITLE.—This Act may be cited as the “Rural Medicare Equity Act of 2007”.

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

Sec. 1. Short title; table of contents.

Sec. 2. Elimination of geographic physician work adjustment factor from geographic indices used to adjust payments under the physician fee schedule.

Sec. 3. Clinical rotation demonstration project.

Sec. 4. Medicare rural health care quality improvement demonstration projects.

Sec. 5. Ensuring proportional representation of interests of rural areas on the Medicare Payment Advisory Commission.

Sec. 6. Implementation of GAO recommendations regarding geographic adjustment indices under the Medicare physician fee schedule.

#### SEC. 2. ELIMINATION OF GEOGRAPHIC PHYSICIAN WORK ADJUSTMENT FACTOR FROM GEOGRAPHIC INDICES USED TO ADJUST PAYMENTS UNDER THE PHYSICIAN FEE SCHEDULE.

(a) FINDINGS.—Congress finds the following:

(1) Variations in the geographic physician work adjustment factors under section 1848(e) of the Social Security Act (42 U.S.C. 1395w-4(e)) result in inequity between localities in payments under the Medicare physician fee schedule.

(2) Beneficiaries under the Medicare program that reside in areas where such adjustment factors are high have relatively more access to services that are paid based on such fee schedule.

(3) There are a number of studies indicating that the market for health care professionals has become nationalized and historically low labor costs in rural and small urban areas have disappeared.

(4) Elimination of the adjustment factors described in paragraph (1) would equalize the reimbursement rate for services reimbursed under the Medicare physician fee schedule while remaining budget-neutral.

(b) ELIMINATION.—Section 1848(e) of the Social Security Act (42 U.S.C. 1395w-4(e)) is amended—

(1) in paragraph (1)(A)(iii), by striking “an index” and inserting “for services provided before January 1, 2008, an index”; and

(2) in paragraph (2), by inserting “, for services provided before January 1, 2008,” after “paragraph (4),” and

(c) BUDGET NEUTRALITY ADJUSTMENT FOR ELIMINATION OF GEOGRAPHIC PHYSICIAN WORK ADJUSTMENT FACTOR.—Section 1848(d) of the Social Security Act (42 U.S.C. 1395w-4(d)), as amended by section 101 of the Medicare Improvement and Extension Act of 2006, is amended—

(1) in paragraph (1)(A), by striking “The conversion” and inserting “Subject to paragraph (8), the conversion”; and

(2) by adding at the end the following new paragraph:

“(8) BUDGET NEUTRALITY ADJUSTMENT FOR ELIMINATION OF GEOGRAPHIC PHYSICIAN WORK ADJUSTMENT FACTOR.—Before applying an update for a year under this subsection, the Secretary shall (if necessary) provide for an adjustment to the conversion factor for that year to ensure that the aggregate payments under this part in that year shall be equal to aggregate payments that would have been made under such part in that year if the amendments made by section 2(b) of the Rural Medicare Equity Act of 2007 had not been enacted.”.

#### SEC. 3. CLINICAL ROTATION DEMONSTRATION PROJECT.

(a) ESTABLISHMENT.—Not later than 6 months after the date of enactment of this Act, the Secretary shall establish a demonstration project that provides for demonstration grants designed to provide finan-

cial or other incentives to hospitals to attract educators and clinical practitioners so that hospitals that serve beneficiaries under the Medicare program under title XVIII of the Social Security Act (42 U.S.C. 1395 et seq.) who are residents of underserved areas may host clinical rotations.

(b) DURATION OF PROJECT.—The demonstration project shall be conducted over a 5-year period.

(c) WAIVER.—The Secretary shall waive such provisions of titles XI and XVIII of the Social Security Act (42 U.S.C. 1301 et seq. and 1395 et seq.) as may be necessary to conduct the demonstration project under this section.

(d) REPORTS.—The Secretary shall submit to the appropriate committees of Congress interim reports on the demonstration project and a final report on such project within 6 months after the conclusion of the project together with recommendations for such legislative or administrative action as the Secretary determines appropriate.

(e) FUNDING.—There are appropriated to the Secretary \$20,000,000 to carry out this section.

(f) DEFINITIONS.—In this section:

(1) HOSPITAL.—The term “hospital” means any subsection (d) hospital (as defined in section 1886(d)(1)(B) of the Social Security Act (42 U.S.C. 1395ww(d)(1)(B))) that had indirect or direct costs of medical education during the most recent cost reporting period preceding the date of enactment of this Act.

(2) SECRETARY.—The term “Secretary” means the Secretary of Health and Human Services.

(3) UNDERSERVED AREA.—The term “underserved area” means such medically underserved urban areas and medically underserved rural areas as the Secretary may specify.

#### SEC. 4. MEDICARE RURAL HEALTH CARE QUALITY IMPROVEMENT DEMONSTRATION PROJECTS.

(a) ESTABLISHMENT.—

(1) IN GENERAL.—Not later than 6 months after the date of enactment of this Act, the Secretary of Health and Human Services (in this section referred to as the “Secretary”) shall establish not more than 10 demonstration projects to provide for improvements, as recommended by the Institute of Medicine, in the quality of health care provided to individuals residing in rural areas.

(2) ACTIVITIES.—Activities under the projects may include public health surveillance, emergency room videoconferencing, virtual libraries, telemedicine, electronic health records, data exchange networks, and any other activities determined appropriate by the Secretary.

(3) CONSULTATION.—The Secretary shall consult with the Rural Health Quality Advisory Commission, the Office of Rural Health Policy of the Health Resources and Services Administration, the Agency for Healthcare Research and Quality, and the Centers for Medicare & Medicaid Services in carrying out the provisions of this section.

(b) DURATION.—Each demonstration project under this section shall be conducted over a 4-year period.

(c) DEMONSTRATION PROJECT SITES.—The Secretary shall ensure that the demonstration projects under this section are conducted at a variety of sites representing the diversity of rural communities in the Nation.

(d) WAIVER.—The Secretary shall waive such provisions of titles XI and XVIII of the Social Security Act (42 U.S.C. 1301 et seq. and 1395 et seq.) as may be necessary to conduct the demonstration projects under this section.

(e) INDEPENDENT EVALUATION.—The Secretary shall enter into an arrangement with

an entity that has experience working directly with rural health systems for the conduct of an independent evaluation of the projects conducted under this section.

(f) **REPORTS.**—The Secretary shall submit to the appropriate committees of Congress interim reports on each demonstration project and a final report on such project within 6 months after the conclusion of the project. Such reports shall include recommendations regarding the expansion of the project to other areas and recommendations for such other legislative or administrative action as the Secretary determines appropriate.

(g) **FUNDING.**—There are appropriated to the Secretary \$50,000,000 to carry out this section.

**SEC. 5. ENSURING PROPORTIONAL REPRESENTATION OF INTERESTS OF RURAL AREAS ON THE MEDICARE PAYMENT ADVISORY COMMISSION.**

(a) **IN GENERAL.**—Section 1805(c)(2) of the Social Security Act (42 U.S.C. 1395b–6(c)(2)) is amended—

(1) in subparagraph (A), by inserting “consistent with subparagraph (E)” after “rural representatives”; and

(2) by adding at the end the following new subparagraph:

“(E) **PROPORTIONAL REPRESENTATION OF INTERESTS OF RURAL AREAS.**—In order to provide a balance between urban and rural representatives under subparagraph (A), the proportion of members who represent the interests of health care providers and Medicare beneficiaries located in rural areas shall be no less than the proportion, of the total number of Medicare beneficiaries, who reside in rural areas.”.

(b) **EFFECTIVE DATE.**—The amendments made by subsection (a) shall apply with respect to appointments made to the Medicare Payment Advisory Commission after the date of the enactment of this Act.

**SEC. 6. IMPLEMENTATION OF GAO RECOMMENDATIONS REGARDING GEOGRAPHIC ADJUSTMENT INDICES UNDER THE MEDICARE PHYSICIAN FEE SCHEDULE.**

Not later than 180 days after the date of enactment of this Act, the Secretary of Health and Human Services shall implement the recommendations contained in the March 2005 GAO report 05–119 entitled “Medicare Physician Fees: Geographic Adjustment Indices are Valid in Design, but Data and Methods Need Refinement.”.

By Mr. SALAZAR (for himself, Mr. MARTINEZ, Mr. MENENDEZ, Mr. BAYH, Mr. BIDEN, Mr. BINGAMAN, Mrs. BOXER, Mr. DOMENICI, Mr. DURBIN, Mrs. FEINSTEIN, Mrs. HUTCHISON, Mr. KENNEDY, Mr. KERRY, Mr. LAUTENBERG, Mr. LIEBERMAN, Mr. LUGAR, Mr. MCCAIN, Mr. NELSON of Florida, Mr. OBAMA, Mr. REID, Mr. SCHUMER, Mr. BROWN, Mr. FEINGOLD, and Mrs. CLINTON):

S. 500. A bill to establish the Commission to Study the Potential Creation of the National Museum of the American Latino to develop a plan of action for the establishment and maintenance of a National Museum of the American Latino in Washington, DC, and for other purposes; to the Committee on Energy and Natural Resources.

Mr. SALAZAR. Mr. President, I rise to speak about bi-partisan legislation I am introducing today. I am proud to be

joined by Senator MEL MARTINEZ, Senator BOB MENENDEZ, and 20 additional Senators from both sides of the aisle.

The National Museum of the American Latino Community Commission Act will establish a Commission to study the potential creation of a National Museum of the American Latino Community. The Commission members, selected by the President and Members of Congress, will be tasked with studying the impact of such a Museum and the cost of constructing and maintaining a museum, developing a plan of action and a fundraising plan, and proposing recommendations to make the Museum a reality.

As we begin our efforts to pass this significant legislation, the U.S. House of Representatives is set to complete their consideration of H.R. 512, the House companion bill, and will pass the bill on the House floor today. It has been a pleasure to working with Representative XAVIER BECERRA and Representative ILEANA ROS-LEHTINEN, who have championed this legislation for several years. I hope to work with the Senate Energy and Natural Resource Committee to quickly advance the Senate bill, so that we can, at last, move forward.

If we are successful in our efforts, I believe we will have done our part to enhance the experience of the millions who visit our Nation's capital every year. By passing this legislation, we will contribute to the ongoing, deeply rewarding, and profoundly important process of national self-discovery.

Washington, DC is the symbolic heart of our country. When Americans travel to their capital, they expect the museums, monuments, and national parks they visit to reflect the complete American experience. I celebrate the opening of the National Museum of the America Indian and efforts underway to establish the National Museum of African American History and Culture because I believe we must celebrate our rich, diverse national heritage.

Hispanics have long been a part of our country's history and my own family's story illustrates this truth.

Over 400 years ago, in 1598, my family helped found the oldest city in what is now these United States. They named the city Santa Fe—the City of Holy Faith—because they knew the hand of God would guide them through the struggles of survival in the ages ahead. In Hispanic Pioneers in Colorado and New Mexico, a new book by Colorado Society of Hispanic Genealogy, their triumph over extreme adversity is documented. The time has come for the story of these pioneers to be told in our Nation's capital.

As a proud American, I want to ensure that every individual who visits Washington has a chance to learn the full history of who we are as Americans. It is my hope that the Senate can work to pass this important bill. In doing so, we will preserve our shared America history.

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

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

S. 500

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

**SECTION 1. SHORT TITLE.**

This Act may be cited as the “Commission to Study the Potential Creation of the National Museum of the American Latino Act of 2007”.

**SEC. 2. ESTABLISHMENT OF COMMISSION.**

(a) **IN GENERAL.**—There is established the Commission to Study the Potential Creation of a National Museum of the American Latino (in this Act referred to as the “Commission”).

(b) **MEMBERSHIP.**—The Commission shall consist of 23 members appointed not later than 6 months after the date of enactment of this Act as follows:

(1) The President shall appoint 7 voting members.

(2) The Speaker of the House of Representatives, the minority leader of the House of Representatives, the majority leader of the Senate, and the minority leader of the Senate shall each appoint 3 voting members.

(3) In addition to the members appointed under paragraph (2), the Speaker of the House of Representatives, the minority leader of the House of Representatives, the majority leader of the Senate, and the minority leader of the Senate shall each appoint 1 nonvoting member.

(c) **QUALIFICATIONS.**—Members of the Commission shall be chosen from among individuals, or representatives of institutions or entities, who possess either—

(1) a demonstrated commitment to the research, study, or promotion of American Latino life, art, history, political or economic status, or culture, together with—

(A) expertise in museum administration;

(B) expertise in fundraising for nonprofit or cultural institutions;

(C) experience in the study and teaching of Latino culture and history at the post-secondary level;

(D) experience in studying the issue of the Smithsonian Institution's representation of American Latino art, life, history, and culture; or

(E) extensive experience in public or elected service; or

(2) experience in the administration of, or the planning for the establishment of, museums devoted to the study and promotion of the role of ethnic, racial, or cultural groups in American history.

**SEC. 3. FUNCTIONS OF THE COMMISSION.**

(a) **PLAN OF ACTION FOR ESTABLISHMENT AND MAINTENANCE OF MUSEUM.**—The Commission shall submit a report to the President and Congress containing its recommendations with respect to a plan of action for the establishment and maintenance of a National Museum of the American Latino in Washington, DC (in this Act referred to as the “Museum”).

(b) **FUNDRAISING PLAN.**—The Commission shall develop a fundraising plan for supporting the creation and maintenance of the Museum through contributions by the American people, and a separate plan on fundraising by the American Latino community.

(c) **REPORT ON ISSUES.**—The Commission shall examine (in consultation with the Secretary of the Smithsonian Institution), and submit a report to the President and Congress on, the following issues:

(1) The availability and cost of collections to be acquired and housed in the Museum.

(2) The impact of the Museum on regional Hispanic- and Latino-related museums.

(3) Possible locations for the Museum in Washington, DC and its environs, to be considered in consultation with the National Capital Planning Commission and the Commission of Fine Arts, the Department of the Interior and Smithsonian Institution.

(4) Whether the Museum should be located within the Smithsonian Institution.

(5) The governance and organizational structure from which the Museum should operate.

(6) How to engage the American Latino community in the development and design of the Museum.

(7) The cost of constructing, operating, and maintaining the Museum.

(d) **LEGISLATION TO CARRY OUT PLAN OF ACTION.**—Based on the recommendations contained in the report submitted under subsection (a) and the report submitted under subsection (c), the Commission shall submit for consideration to the Committee on Transportation and Infrastructure of the House of Representatives, the Committee on House Administration of the House of Representatives, the Committee on Rules and Administration of the Senate, the Committees on Natural Resources of the House of Representatives and the Senate, and the Committees on Appropriations of the House of Representatives and the Senate recommendations for a legislative plan of action to create and construct the Museum.

(e) **NATIONAL CONFERENCE.**—In carrying out its functions under this section, the Commission may convene a national conference on the Museum, comprised of individuals committed to the advancement of American Latino life, art, history, and culture, not later than 18 months after the commission members are selected.

#### **SEC. 4. ADMINISTRATIVE PROVISIONS.**

(a) **FACILITIES AND SUPPORT OF DEPARTMENT OF THE INTERIOR.**—The Department of the Interior shall provide from funds appropriated for this purpose administrative services, facilities, and funds necessary for the performance of the Commission's functions. These funds shall be made available prior to any meetings of the Commission.

(b) **COMPENSATION.**—Each member of the Commission who is not an officer or employee of the Federal Government may receive compensation for each day on which the member is engaged in the work of the Commission, at a daily rate to be determined by the Secretary of the Interior.

(c) **TRAVEL EXPENSES.**—Each member shall be entitled to travel expenses, including per diem in lieu of subsistence, in accordance with applicable provisions under subchapter I of chapter 57 of title 5, United States Code.

(d) **FEDERAL ADVISORY COMMITTEE ACT.**—The Commission is not subject to the provisions of the Federal Advisory Committee Act.

#### **SEC. 5. DEADLINE FOR SUBMISSION OF REPORTS; TERMINATION.**

(a) **DEADLINE.**—The Commission shall submit final versions of the reports and plans required under section 3 not later than 24 months after the date of the Commission's first meeting.

(b) **TERMINATION.**—The Commission shall terminate not later than 30 days after submitting the final versions of reports and plans pursuant to subsection (a).

#### **SEC. 6. AUTHORIZATION OF APPROPRIATIONS.**

There are authorized to be appropriated for carrying out the activities of the Commission \$2,100,000 for the first fiscal year beginning after the date of enactment of this Act and \$1,100,000 for the second fiscal year beginning after the date of enactment of this Act.

By Mr. SMITH:

S. 504. A bill to amend the Internal Revenue Code of 1986 to establish long-term care trust accounts and allow a refundable tax credit for contributions to such accounts, and for other purposes; to the Committee on Finance.

Mr. SMITH. Mr. President, I rise today to introduce the Long-Term Care Trust Account Act of 2007. I am pleased to be joined by my colleague Senator BLANCHE LINCOLN who has been a tireless leader on issues of importance to the health of our Nation. I look forward to continuing to work with Senator LINCOLN on this legislation as well as other opportunities to improve health care in America.

We are an aging Nation. With babyboomers rapidly retiring, the need for long-term care planning is becoming even more critical. However, we know all too well that planning for the likelihood of disability in young or old age is not done as actively as we would like it to be. Currently, only about 7 percent of all money spent on long-term care comes from private insurance. Too often, insurance is not being purchased, funds are not being saved and persons with disabilities are forced to rely on Medicaid for their daily care.

As a Nation, we need to do better. Senator LINCOLN and I believe that our bill will encourage Americans to invest in their futures and in their care, which is an important first step.

Specifically, our legislation will create a new type of savings mechanism for the purpose of preparing for the costs associated with long-term care services and purchasing long-term care insurance. An individual who establishes a long-term care trust account can contribute up to \$5,000 per year to their account and receive a refundable 10 percent tax credit on that contribution. Interest accrued on these accounts will be tax free, and funds could be withdrawn for the purchase of long-term care insurance or to pay for long-term care services. Our bill also will allow an individual to make contributions to another person's Long-Term Care Trust Account. This will allow relatives to help their parents or a loved one prepare for their future health care needs.

The Centers for Medicare and Medicaid Services estimates that national spending for long-term care was more than \$190 billion in 2004, representing about 12.5 percent of all personal health care expenditures. While those numbers already are staggering, we also know that the need for long-term care is expected to grow significantly in coming decades. Almost two-thirds of people receiving long-term care are over age 65, with this number expected to double by 2030. We also know that the population over age 85, those most likely to need long-term services and supports, is expected to increase more than 250 percent by 2040 from 4.3 million to 15.4 million.

Today, millions of Americans are receiving or are in need of long-term care

services and supports. Surprisingly, more than 40 percent of persons receiving long-term care are between the ages of 18 and 64. Some were born with disabilities; others came to be disabled through accident or illness. No one can predict their long-term health care needs. Therefore, everyone needs to be prepared.

Currently, long-term care insurance is the main way to prepare for possible future care and support needs. Long-term care insurance helps protect assets and income from the devastating financial consequences of long-term health care costs. Today's comprehensive long-term care insurance policies allow consumers to choose from a variety of benefits and offer a wide range of coverage choices. They allow individuals to receive care in a variety of settings including nursing homes, home care, assisted living facilities and adult day care. Some of the most recent policies also provide a cash-benefit that a consumer can spend in the manner he or she chooses. When we buy long-term care insurance, we are also working to ensure that we can make more independent long-term care decisions and reduce the strain on state Medicaid budgets.

Unfortunately, for too many, the struggle to pay the immediate costs of long-term care insurance sometimes outweighs the security these products would provide. As Americans are spending more and saving less, I fear the American middle class is woefully unprepared to meet the coming challenges of their long-term care needs. Moving forward in our effort to help individuals prepare for life in their later years, we must encourage them to purchase long-term care insurance and save for long-term care services. The Long-Term Care Trust Account Act of 2007 is designed to achieve both goals.

It is my hope that this legislation will help all Americans save for their future and their independence during times of vulnerability. I urge my colleagues on both sides of the aisle to support this important bill.

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

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

S. 504

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

#### **SECTION 1. SHORT TITLE.**

This Act may be cited as the "Long-Term Care Trust Account Act of 2007".

#### **SEC. 2. LONG-TERM CARE TRUST ACCOUNTS.**

(a) **IN GENERAL.**—Subchapter F of chapter 1 of the Internal Revenue Code of 1986 (relating to exempt organizations) is amended by adding at the end the following new part:

#### **"PART IX—LONG-TERM CARE TRUST ACCOUNTS**

#### **"SEC. 530A. LONG-TERM CARE TRUST ACCOUNTS.**

"(a) **GENERAL RULE.**—A Long-Term Care Trust Account shall be exempt from taxation



under this subtitle. Notwithstanding the preceding sentence, such account shall be subject to the taxes imposed by section 511 (relating to imposition of tax on unrelated business income of charitable organizations).

“(b) **LONG-TERM CARE TRUST ACCOUNT.**—For purposes of this section, the term ‘Long-Term Care Trust Account’ means a trust created or organized in the United States for the exclusive benefit of an individual who is the designated beneficiary of the trust and which is designated (in such manner as the Secretary shall prescribe) at the time of the establishment of the trust as a Long-Term Care Trust Account, but only if the written governing instrument creating the trust meets the following requirements:

“(1) Except in the case of a qualified rollover contribution described in subsection (d)—

“(A) no contribution will be accepted unless it is in cash, and

“(B) contributions will not be accepted for the calendar year in excess of the contribution limit specified in subsection (c)(1).

“(2) The trustee is a bank (as defined in section 408(n)), an insurance company (as defined in section 816), or another person who demonstrates to the satisfaction of the Secretary that the manner in which that person will administer the trust will be consistent with the requirements of this section or who has so demonstrated with respect to any individual retirement plan.

“(3) No part of the trust assets will be invested in life insurance contracts.

“(4) The interest of an individual in the balance of his account is nonforfeitable.

“(5) The assets of the trust shall not be commingled with other property except in a common trust fund or common investment fund.

“(6) Except as provided in subsection (e)(2), no distribution will be allowed if at the time of such distribution the designated beneficiary is not a chronically ill individual (as defined in section 7702B(c)(2)).

“(c) **TAX TREATMENT OF CONTRIBUTIONS.**—

“(1) **CONTRIBUTION LIMIT.**—

“(A) **IN GENERAL.**—The aggregate amount of contributions (other than qualified rollover contributions described in subsection (d)) for any taxable year to all Long-Term Care Trust Accounts maintained for the benefit of the designated beneficiary shall not exceed \$5,000.

“(B) **INFLATION ADJUSTMENT.**—In the case of any taxable year beginning in a calendar year after 2007, the dollar amount under subparagraph (A) shall be increased by an amount equal to—

“(i) such dollar amount, multiplied by

“(ii) the medical care cost adjustment determined under section 213(d)(10)(B)(ii) for the calendar year in which the taxable year begins, determined by substituting ‘2006’ for ‘1996’ in subclause (II) thereof.

If any amount as adjusted under the preceding sentence is not a multiple of \$10, such amount shall be rounded to the next lowest multiple of \$10.

“(2) **GIFT TAX TREATMENT OF CONTRIBUTIONS.**—For purposes of chapters 12 and 13—

“(A) **IN GENERAL.**—Any contribution to a Long-Term Care Trust Account on behalf of any designated beneficiary—

“(i) shall be treated as a completed gift to such beneficiary which is not a future interest in property, and

“(ii) shall not be treated as a qualified transfer under section 2503(e).

“(B) **TREATMENT OF EXCESS CONTRIBUTIONS.**—If the aggregate amount of contributions described in subparagraph (A) during the calendar year by a donor exceeds the limitation for such year under section 2503(b), such aggregate amount shall, at the

election of the donor, be taken into account for purposes of such section ratably over the 5-year period beginning with such calendar year.

“(d) **QUALIFIED ROLLOVER CONTRIBUTION.**—For purposes of this section, the term ‘qualified rollover contribution’ means a contribution to a Long-Term Care Trust Account—

“(1) from another such account of the same beneficiary, but only if such amount is contributed not later than the 60th day after the distribution from such other account, and

“(2) from a Long-Term Care Trust Account of a spouse of the beneficiary of the account to which the contribution is made, but only if such amount is contributed not later than the 60th day after the distribution from such other account.

“(e) **TAX TREATMENT OF DISTRIBUTIONS.**—

“(1) **IN GENERAL.**—Any distribution from a Long-Term Care Trust Account shall be includible in the gross income of the distributee in the manner as provided under section 72 to the extent not excluded from gross income under any other provision of this subsection.

“(2) **LONG-TERM CARE INSURANCE PREMIUMS.**—If at the time of any distribution, the designated beneficiary is not a chronically ill individual (as defined in section 7702B(c)(2)), no amount shall be includible in gross income under paragraph (1) if the aggregate premiums for any qualified long-term care insurance contract for such beneficiary during the taxable year are not less than the aggregate distributions during the taxable year.

“(3) **DISTRIBUTIONS FOR QUALIFIED LONG-TERM CARE SERVICES.**—For purposes of this subsection, if at the time of any distribution, the designated beneficiary is a chronically ill individual (as so defined)—

“(A) **IN-KIND DISTRIBUTIONS.**—No amount shall be includible in gross income under paragraph (1) by reason of a distribution which consists of providing a benefit to the distributee which, if paid for by the distributee, would constitute expenses for any qualified long-term care services (as defined in section 7702B(c)).

“(B) **CASH DISTRIBUTIONS.**—In the case of distributions not described in subparagraph (A), if—

“(i) such distributions do not exceed the expenses for qualified long-term care services (as so defined), reduced by expenses described in subparagraph (A), no amount shall be includible in gross income, and

“(ii) in any other case, the amount otherwise includible in gross income shall be reduced by an amount which bears the same ratio to such amount as such expenses bear to such distributions.

“(4) **CHANGE IN BENEFICIARIES OR ACCOUNTS.**—Paragraph (1) shall not apply to that portion of any distribution which, within 60 days of such distribution, is transferred—

“(A) to another Long-Term Care Trust Account for the benefit of the designated beneficiary, or

“(B) to the credit of another designated beneficiary under a Long-Term Care Trust Account who is a spouse of the designated beneficiary with respect to which the distribution was made.

“(5) **OPERATING RULES.**—For purposes of applying section 72—

“(A) to the extent provided by the Secretary, all Long-Term Care Trust Accounts of which an individual is a designated beneficiary shall be treated as one account,

“(B) except to the extent provided by the Secretary, all distributions during a taxable year shall be treated as one distribution, and

“(C) except to the extent provided by the Secretary, the value of the contract, income on the contract, and investment in the con-

tract shall be computed as of the close of the calendar year in which the taxable year begins.

“(6) **SPECIAL RULES FOR DEATH AND DIVORCE.**—

“(A) **IN GENERAL.**—Rules similar to the rules of paragraphs (7) and (8) of section 220(f) shall apply.

“(B) **AMOUNTS INCLUDIBLE IN ESTATE OF DONOR MAKING EXCESS CONTRIBUTIONS.**—In the case of a donor who makes the election described in subsection (c)(2)(B) and who dies before the close of the 5-year period referred to in such subsection, the gross estate of the donor shall include the portion of such contributions properly allocable to periods after the date of death of the donor.

“(7) **ADDITIONAL TAX.**—The tax imposed by this chapter for any taxable year on any taxpayer who receives a payment or distribution from a Long-Term Care Trust Account which is includible in gross income shall be increased by 25 percent of the amount which is so includible under rules similar to the rules of section 530(d)(4).

“(8) **DENIAL OF DOUBLE BENEFIT.**—For purposes of determining the amount of any deduction under this chapter, any payment or distribution out of a Long-Term Care Trust Account shall not be treated as an expense paid for medical care.

“(f) **DESIGNATED BENEFICIARY.**—For purposes of this section, the term ‘designated beneficiary’ means the individual designated at the commencement of participation in the Long-Term Care Trust Account as the beneficiary of amounts paid (or to be paid) to the account.

“(g) **LOSS OF TAXATION EXEMPTION OF ACCOUNT WHERE BENEFICIARY ENGAGES IN PROHIBITED TRANSACTION.**—Rules similar to the rules of paragraph (2) of section 408(e) shall apply to any Long-Term Care Trust Account.

“(h) **CUSTODIAL ACCOUNTS.**—For purposes of this section, a custodial account or an annuity contract issued by an insurance company qualified to do business in a State shall be treated as a trust under this section if—

“(1) the custodial account or annuity contract would, except for the fact that it is not a trust, constitute a trust which meets the requirements of subsection (b), and

“(2) in the case of a custodial account, the assets of such account are held by a bank (as defined in section 408(n)) or another person who demonstrates, to the satisfaction of the Secretary, that the manner in which he will administer the account will be consistent with the requirements of this section.

For purposes of this title, in the case of a custodial account or annuity contract treated as a trust by reason of the preceding sentence, the person holding the assets of such account or holding such annuity contract shall be treated as the trustee thereof.

“(i) **REPORTS.**—The trustee of a Long-Term Care Trust Account shall make such reports regarding such account to the Secretary and to the beneficiary of the account with respect to contributions, distributions, and such other matters as the Secretary may require. The reports required by this subsection shall be filed at such time and in such manner and furnished to such individuals at such time and in such manner as may be required.”

(b) **TAX ON EXCESS CONTRIBUTIONS.**—

(1) **IN GENERAL.**—Subsection (a) of section 4973 of the Internal Revenue Code of 1986 (relating to tax on excess contributions to certain tax-favored accounts and annuities) is amended by striking “or” at the end of paragraph (4), by inserting “or” at the end of paragraph (5), and by inserting after paragraph (5) the following new paragraph:

“(6) a Long-Term Care Trust Account (as defined in section 530A).”

(2) EXCESS CONTRIBUTION.—Section 4973 of such Code is amended by adding at the end the following new subsection:

“(h) EXCESS CONTRIBUTIONS TO LONG-TERM CARE TRUST ACCOUNTS.—For purposes of this section—

“(1) IN GENERAL.—In the case of Long-Term Care Trust Accounts (within the meaning of section 530A), the term ‘excess contributions’ means the sum of—

“(A) the amount by which the amount contributed for the calendar year to such accounts (other than qualified rollover contributions (as defined in section 530A(d))) exceeds the contribution limit under section 530A(c)(1), and

“(B) the amount determined under this subsection for the preceding calendar year, reduced by the excess (if any) of the maximum amount allowable as a contribution under section 530A(c)(1) for the calendar year over the amount contributed to the accounts for the calendar year.

“(2) SPECIAL RULE.—A contribution shall not be taken into account under paragraph (1) if such contribution (together with the amount of net income attributable to such contribution) is returned to the beneficiary before June 1 of the year following the year in which the contribution is made.”.

(c) FAILURE TO PROVIDE REPORTS ON LONG-TERM CARE TRUST ACCOUNTS.—Paragraph (2) of section 6693(a) of the Internal Revenue Code of 1986 (relating to failure to provide reports on individual retirement accounts or annuities) is amended by striking “and” at the end of subparagraph (D), by striking the period at the end of subparagraph (E) and inserting “, and”, and by inserting after subparagraph (E) the following new subparagraph:

“(F) section 530A(i) (relating to Long-Term Care Trust Accounts).”.

(d) CONFORMING AMENDMENT.—The table of parts for subchapter F of chapter 1 of the Internal Revenue Code of 1986 is amended by adding at the end the following new item:

“PART IX. LONG-TERM CARE TRUST ACCOUNTS”.

(e) EFFECTIVE DATE.—The amendments made by this section shall apply to taxable years beginning after December 31, 2006.

**SEC. 3. REFUNDABLE CREDIT FOR CONTRIBUTIONS TO LONG-TERM CARE TRUST ACCOUNTS.**

(a) IN GENERAL.—Subpart C of part IV of subchapter A of chapter 1 of the Internal Revenue Code of 1986 (relating to refundable credits) is amended by inserting after section 35 the following new section:

**“SEC. 35A. CONTRIBUTIONS TO LONG-TERM CARE TRUST ACCOUNTS.**

“(a) GENERAL RULE.—In the case of an individual, there shall be allowed as a credit against the tax imposed by this subtitle for the taxable year an amount equal to 10 percent of the contributions to any Long-Term Care Trust Account allowed under section 530A for such taxable year.

“(b) REDUCTION BASED ON ADJUSTED GROSS INCOME.—

“(1) IN GENERAL.—The percentage which would (but for this subsection) be taken into account under subsection (a) for the taxable year shall be reduced (but not below zero) by the percentage determined under paragraph (2).

“(2) AMOUNT OF REDUCTION.—The percentage determined under this paragraph is the percentage which bears the same ratio to the percentage which would be so taken into account as—

“(A) the excess of—

“(i) the taxpayer’s adjusted gross income for such taxable year, over

“(ii) \$95,000 (\$190,000 in the case of a joint return), bears to

“(B) \$10,000 (\$20,000 in the case of a joint return).

“(3) ADJUSTED GROSS INCOME.—For purposes of this subsection, adjusted gross income shall be determined without regard to sections 911, 931, and 933.

“(c) DENIAL OF DOUBLE BENEFIT.—No deduction shall be allowed under this chapter for any amount taken into account in determining the credit under this section.”.

(b) CONFORMING AMENDMENTS.—

(1) Paragraph (2) of section 1324(b) of title 31, United States Code, is amended by inserting before the period “, or from section 35A of such Code”.

(2) The table of sections of subpart C of part IV of subchapter A of chapter 1 of the Internal Revenue Code of 1986 is amended by inserting after the item relating to section 35 the following new item:

“Sec. 35A. Contributions to Long-Term Care Trust Accounts.”.

(c) EFFECTIVE DATE.—The amendments made by this section shall apply to amounts paid or incurred in taxable years beginning after December 31, 2005.

By Ms. COLLINS (for herself, Mr. WARNER, Ms. LANDRIEU, Mr. COLEMAN, Mr. VITTER, Mr. SMITH, and Mr. NELSON of Nebraska).

S. 505. A bill to amend the Internal Revenue Code of 1986 to increase the above-the-line deduction for teacher classroom supplies and to expand such deduction to include qualified professional development expenses; to the Committee on Finance.

Ms. COLLINS. Mr. President, the bill that I am introducing today, along with Senators WARNER, LANDRIEU, VITTER, COLEMAN, SMITH, and NELSON of Nebraska, would increase and expand the Teacher Tax deduction provided in current law. The Teacher Tax deduction is available to school teachers and other educators who incur out-of-pocket expenses in order to purchase classroom supplies for their students. The bill we are offering today would increase this above-the-line tax deduction to \$400, allow the deduction to be taken for expenses related to professional development, and make the deduction permanent.

This bill builds upon a \$250 tax deduction in current law authored by Senator WARNER and myself, which became law as part of the tax relief package in 2001. This tax relief was later extended through the end of this year, but we need to act to extend it further.

I would suggest that there is no reason why we should not make the deduction permanent. Teachers who buy classroom supplies in order to improve the educational experience of their students deserve more than just our gratitude. They deserve this modest tax relief to thank them for their hard work.

So often teachers in my State, and throughout the country, spend their own money in order to improve the classroom experiences of their students. Many of us are familiar with a survey of the National Education Association that found that teachers spend, on average, \$443 a year on classroom supplies. Other surveys show that they are spending even more than that. In

fact, the National School Supply and Equipment Association found that educators spend an average of \$826 to supplement classroom supplies, plus \$926 for instructional materials on top of that—for a total of over \$1,700 out of their own pockets.

In most States, including mine, teachers are very modestly paid for their jobs. I think it is so impressive that despite challenging jobs and modest salaries, teachers are willing to dig deep into their own pockets to enrich the classroom experience, because they care so deeply for their students.

Indeed, I have spoken to dozens of teachers in Maine who tell me they routinely spend far in excess of the \$250 deduction limit that is in current law. I have made a practice of visiting schools all over Maine, and so far, I have had the opportunity to visit more than 160 schools in my State. At virtually every school I visit, I find teachers who are spending their own money to benefit their students. Year after year, these teachers spend hundreds of dollars on books, bulletin boards, computer software, crayons, construction paper, stamps, inkpads—everything you can think of. Let me just give you a couple of examples. Anita Hopkins and Kathi Toothaker, who are elementary school teachers from Augusta, ME, purchase books for their students to have as a classroom library, as well as workbooks and sight cards. They have also purchased special prizes for positive reinforcement for their students. Mrs. Hopkins estimates that she spends \$800 to \$1,000 of her own money on extra materials to make learning fun and to create a stimulating classroom environment.

This bill would also expand the Teacher Tax deduction to make it available to teachers who incur expenses for professional development. Whenever the provisions of “No Child Left Behind” are being debated, we hear a lot of discussion about the need for highly-qualified teachers. One of the best ways for teachers to improve their qualifications is through professional development. Yet, in towns in my State, and I suspect throughout the country, school budgets are often very tight, and money for professional development is either very limited or non-existent. For that reason, I believe we should allow this tax deduction to also apply when a teacher takes a course or attends a workshop and has to pay for it out of his or her own pocket.

In my view, students are the ultimate beneficiaries when teachers receive professional development to sharpen their skills or to learn a new approach to presenting material to their students. Studies have consistently shown that, other than involved parents, the single greatest determinant of classroom success is the presence of a well-qualified teacher. Educators themselves understand just how important professional development is to their ability to make a positive impact in the classroom.

The Teacher Tax relief that we have made available since 2001 is certainly a positive step, and I was proud to have authored that law, along with Senator WARNER. This bill would increase that deduction from \$250 to \$400, reflecting more accurately what teachers really spend, and would make the deduction permanent. The National Education Association has endorsed this bill, and I ask unanimous consent that a copy of the NEA's letter be printed in the RECORD at the end of my statement.

This bill is a small but appropriate means of recognizing the many sacrifices that our teachers make every day to benefit the children of America. I urge my colleagues to support it.

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

NATIONAL EDUCATION ASSOCIATION,  
Washington, DC, January 24, 2007.

Senator SUSAN COLLINS,  
Senator JOHN WARNER,  
U.S. Senate,  
Washington, DC.

DEAR SENATORS COLLINS AND WARNER: On behalf of the National Education Association's, NEA, 3.2 million members, we would like to express our strong support for your legislation that would increase, expand, and make permanent the tax deduction for educators' out-of-pocket classroom supply expenses. We thank you for your continued leadership and advocacy on this important issue.

As you know, the educator tax deduction helps recognize the financial sacrifices made by teachers and paraprofessionals, who often reach into their own pockets to purchase classroom supplies such as books, pencils, paper, and art supplies. Studies show that teachers are spending more of their own funds each year to supply their classrooms, including purchasing essential items such as pencils, glue, scissors, and facial tissues. For example, NEA's 2003 report Status of the American Public School Teacher, 2000-2001 found that teachers spent an average of \$443 a year on classroom supplies. More recently, the National School Supply and Equipment Association found that in 2005-2006, educators spent out of their own pockets an average of \$826.00 for supplies and an additional \$926 for instructional materials, for a total of \$1,752.

By increasing the current deduction and making it permanent, your legislation will make a real difference for many educators, who often must sacrifice other personal needs in order to pay for classroom supplies.

NEA also strongly supports your proposal to extend the tax deduction to cover out-of-pocket professional development expenses. Teacher quality is the single most critical factor in maximizing student achievement. Ongoing professional development is essential to ensure that educators stay up-to-date on the skills and knowledge necessary to prepare students for the challenges of the 21st century. Your bill will make a critical difference in helping educators access quality training.

We thank you again for your work on this important legislation and look forward to continuing to work with you to support our nation's educators.

Sincerely,

DIANE SHUST,  
Director of Govern-  
ment Relations.  
RANDALL MOODY,  
Manager, Policy and  
Politics.

Mr. WARNER. Mr. President, I rise today in support, once again, of America's teachers by joining with Senator COLLINS in introducing legislation regarding the Teacher Tax Relief Act.

Senator COLLINS and I have worked closely for some time now in support of legislation to provide our teachers with tax relief in recognition of the many out-of-pocket expenses they incur as part of their profession. In the 107th Congress, we were successful in providing much needed tax relief for our Nation's teachers with passage of H.R. 3090, the "Job Creation and Worker Assistance Act of 2002."

This legislation, which was signed into law by President Bush, included the Collins/Warner "Teacher Tax Relief Act of 2001" provisions that provided a \$250 above the line deduction for educators who incur out-of-pocket expenses for supplies they bring into the classroom to better the education of their students. These important provisions provided almost half a billion dollars worth of tax relief to teachers all across America in 2002 and 2003.

In the 108th Congress we were able to successfully extend the provisions of the Teacher Tax Relief Act for 2004 and 2005. In the 109th Congress we were able to successfully extend the provisions for 2006 and 2007.

While these provisions will provide substantial relief to America's teachers, our work is not yet complete.

It is now estimated that the average teacher spends \$826 out of their own pocket each year on classroom materials—materials such as pens, pencils and books. First year teachers spend even more.

Why do they do this? Simply because school budgets are not adequate to meet the costs of education. Our teachers dip into their own pocket to better the education of America's youth.

Moreover, in addition to spending substantial money on classroom supplies, many teachers spend even more money out of their own pocket on professional development. Such expenses include tuition, fees, books, and supplies associated with courses that help our teachers become even better instructors.

The fact is that these out-of-pocket costs place lasting financial burdens on our teachers. This is one reason our teachers are leaving the profession. Little wonder that our country is in the midst of a teacher shortage.

Without a doubt the Teacher Tax Relief Act of 2001 took a step forward in helping to alleviate the Nation's teaching shortage by providing a \$250 above the line deduction for classroom expenses.

However, it is clear that our teachers are spending much more than \$250 a year out of their own pocket to better the education of our children.

Accordingly, Senator COLLINS and I have joined together to take another step forward by introducing this legislation.

This proposed legislation will build upon current law in three ways. The

legislation will: One, increase the above-the-line deduction, as President Bush has called for, from \$250 allowed under current law to \$400; two, allow educators to include professional development costs within that \$400 deduction. Under current law, up to \$250 is deductible but only for classroom expenses; and three, make the Teacher Tax Relief provisions in the law permanent. Current law sunsets the Collins/Warner provisions after 2007.

Our teachers have made a personal commitment to educate the next generation and to strengthen America. And, in my view, the Federal Government should recognize the many sacrifices our teachers make in their career.

This Teacher Tax Relief Act is another step forward in providing our educators with the recognition they deserve.

By Mr. LAUTENBERG (for himself, Ms. SNOWE, and Mrs. BOXER):

S. 506. A bill to improve efficiency in the Federal Government through the use of high-performance green buildings, and for other purposes; to the committee on Environment and Public Works.

Mr. LAUTENBERG. Mr. President, I am pleased to be joined by my colleagues, Senators SNOWE and BOXER, to introduce the High Performance Green Buildings Act. This legislation encourages the government to improve the energy efficiency, indoor air quality, and environmental impacts of our Nation's Federal buildings, and will re-energize and focus the Federal Government's leadership and commitment on this issue.

Buildings in the United States have an enormous impact on the environment and also on our overall energy situation. According to the Department of Energy, buildings in the United States use almost 40 percent of the total energy consumed in this country. That figure is expected to rise to 53 percent by 2030, meaning that over half of the energy consumed in this country will be used by buildings alone. In addition, buildings are the source of 35 percent of national carbon dioxide emissions, 49 percent of sulfur dioxide emissions, and 25 percent of nitrogen oxide emissions.

However, the impact of buildings is even broader than that. Americans spend approximately 90 percent of their time indoors and the quality of the air they breathe can have an impact on their health, as well as work productivity and absenteeism. The U.S. Green Buildings Council, a national non-profit, indicates that on average, installing high performance lighting enhances worker productivity by 6.7 percent. There are also numerous sources of indoor air pollutants, ranging from mold to radon, and strong building design that considers ventilation can help to remedy these potential health problems.

It is important that we confront these issues, and our legislation does just that. High Performance Green Buildings are designed with the impact on occupants, surroundings and energy consumption in mind. Buildings designed or renovated on these merits save money, have healthier occupants, and have a more positive impact on their communities.

While the initial investment cost of green buildings may be higher than a traditional building, many of these costs are recouped over time. For instance, the Federal government spends about \$170 million per year on the lighting of federal buildings; using new lighting technology can reduce energy use by 50 to 75 percent. Some estimates show that the payback time for energy efficient lighting is as little as four months.

The High Performance Green Buildings Act focuses the Federal Government's efforts on promoting sustainable design in federal buildings, and realizing the economic benefits associated with reduced energy use and increased occupant health. It creates an Office of High Performance Green Buildings within the General Services Administration (GSA), which manages buildings owned or leased by the Federal Government. GSA is the largest "landlord" in the country the government owns or leases nearly 500,000 buildings in the United States, covering 3.1 billion square feet. The new Office will promote public outreach, focus ongoing research and development, and create an Advisory Committee consisting of Agency representatives and experts from various sectors, to improve coordination across Federal Government agencies and bring best practices to the Federal government.

Additionally, the High Performance Green Buildings Act provides grants to schools, in consultation with the Environmental Protection Agency and the Department of Education, to provide technical assistance to address environmental and health concerns. The health of our children is our primary concern and this legislation takes important steps to ensure their well-being.

It is clear that having sustainable design in our buildings is smart public policy and a wise financial investment, and this bill will allow the Federal Government to increase its leadership role on the promotion of green buildings. I urge my colleagues to support this bill.

I ask unanimous consent that the full text of the bill be printed in the RECORD.

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

S. 506

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

#### SECTION 1. SHORT TITLE; TABLE OF CONTENTS.

(a) SHORT TITLE.—This Act may be cited as the "High-Performance Green Buildings Act of 2007".

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

Sec. 1. Short title; table of contents.

Sec. 2. Definitions.

#### TITLE I—OFFICE OF HIGH-PERFORMANCE GREEN BUILDINGS

Sec. 101. Oversight.

Sec. 102. Office of High-Performance Green Buildings.

Sec. 103. Green Building Advisory Committee.

Sec. 104. Public outreach.

Sec. 105. Research and development.

Sec. 106. Budget and life-cycle costing and contracting.

Sec. 107. Authorization of appropriations.

#### TITLE II—HEALTHY HIGH-PERFORMANCE SCHOOLS

Sec. 201. Definition of high-performance school.

Sec. 202. Grants for healthy school environments.

Sec. 203. Model guidelines for siting of school facilities.

Sec. 204. Public outreach.

Sec. 205. Environmental health program.

Sec. 206. Authorization of appropriations.

#### TITLE III—STRENGTHENING FEDERAL LEADERSHIP

Sec. 301. Incentives.

Sec. 302. Federal procurement.

Sec. 303. Federal green building performance.

#### TITLE IV—DEMONSTRATION PROJECT

Sec. 401. Coordination of goals.

Sec. 402. Authorization of appropriations.

#### SEC. 2. DEFINITIONS.

In this Act:

(1) ADMINISTRATOR.—The term "Administrator" means the Administrator of General Services.

(2) COMMITTEE.—The term "Committee" means the Green Building Advisory Committee established under section 103(a).

(3) DIRECTOR.—The term "Director" means the individual appointed to the position established under section 101(a).

(4) FEDERAL FACILITY.—

(A) IN GENERAL.—The term "Federal facility" means any building or facility the intended use of which requires the building or facility to be—

(i) accessible to the public; and

(ii) constructed or altered by or on behalf of the United States.

(B) EXCLUSIONS.—The term "Federal facility" does not include a privately-owned residential or commercial structure that is not leased by the Federal Government.

(5) HIGH-PERFORMANCE GREEN BUILDING.—The term "high-performance green building" means a building—

(A) that, during its life-cycle—

(i) reduces energy, water, and material resource use and the generation of waste;

(ii) improves indoor environmental quality, including protecting indoor air quality during construction, using low-emitting materials, improving thermal comfort, and improving lighting and acoustic environments that affect occupant health and productivity;

(iii) improves indoor and outdoor impacts of the building on human health and the environment;

(iv) increases the use of environmentally preferable products, including biobased, recycled content, and nontoxic products with lower life-cycle impacts;

(v) increases reuse and recycling opportunities; and

(vi) integrates systems in the building; and (B) for which, during its planning, design, and construction, the environmental and energy impacts of building location and site design are considered.

(6) LIFE CYCLE.—The term "life cycle", with respect to a high-performance green building, means all stages of the useful life of the building (including components, equipment, systems, and controls of the building) beginning at conception of a green building project and continuing through site selection, design, construction, landscaping, commissioning, operation, maintenance, renovation, deconstruction or demolition, removal, and recycling of the green building.

(7) LIFE-CYCLE ASSESSMENT.—The term "life-cycle assessment" means a comprehensive system approach for measuring the environmental performance of a product or service over the life of the product or service, beginning at raw materials acquisition and continuing through manufacturing, transportation, installation, use, reuse, and end-of-life waste management.

(8) LIFE-CYCLE COSTING.—The term "life-cycle costing", with respect to a high-performance green building, means a technique of economic evaluation that—

(A) sums, over a given study period, the costs of initial investment (less resale value), replacements, operations (including energy use), and maintenance and repair of an investment decision; and

(B) is expressed—

(i) in present value terms, in the case of a study period equivalent to the longest useful life of the building, determined by taking into consideration the typical life of such a building in the area in which the building is to be located; or

(ii) in annual value terms, in the case of any other study period.

(9) OFFICE.—The term "Office" means the Office of High-Performance Green Buildings established under section 102(a).

#### TITLE I—OFFICE OF HIGH-PERFORMANCE GREEN BUILDINGS

##### SEC. 101. OVERSIGHT.

(a) IN GENERAL.—The Administrator shall establish within the General Services Administration, and appoint an individual to serve as Director in, a position in the career-reserved Senior Executive service, to—

(1) establish and manage the Office in accordance with section 102; and

(2) carry out other duties as required under this Act.

(b) COMPENSATION.—The compensation of the Director shall not exceed the maximum rate of basic pay for the Senior Executive Service under section 5382 of title 5, United States Code, including any applicable locality-based comparability payment that may be authorized under section 5304(h)(2)(C) of that title.

##### SEC. 102. OFFICE OF HIGH-PERFORMANCE GREEN BUILDINGS.

(a) ESTABLISHMENT.—The Director shall establish within the General Services Administration an Office of High-Performance Green Buildings.

(b) DUTIES.—The Director shall—

(1) ensure full coordination of high-performance green building information and activities within the General Services Administration and all relevant Federal agencies, including, at a minimum—

(A) the Environmental Protection Agency;

(B) the Office of the Federal Environmental Executive;

(C) the Office of Federal Procurement Policy;

(D) the Department of Energy;

(E) the Department of Health and Human Services;

(F) the Department of Defense; and

(G) such other Federal agencies as the Director considers to be appropriate;

(2) establish a senior-level green building advisory committee, which shall provide advice and recommendations in accordance with section 103;

(3) identify and biennially reassess improved or higher rating standards recommended by the Committee;

(4) establish a national high-performance green building clearinghouse in accordance with section 104, which shall provide green building information through—

(A) outreach;

(B) education; and

(C) the provision of technical assistance;

(5) ensure full coordination of research and development information relating to high-performance green building initiatives under section 105;

(6) identify and develop green building standards that could be used for all types of Federal facilities in accordance with section 105;

(7) establish green practices that can be used throughout the life of a Federal facility;

(8) review and analyze current Federal budget practices and life-cycle costing issues, and make recommendations to Congress, in accordance with section 106; and

(9) complete and submit the report described in subsection (c).

(c) **REPORT.**—Not later than 2 years after the date of enactment of this Act, and biennially thereafter, the Director shall submit to Congress a report that—

(1) describes the status of the green building initiatives under this Act and other Federal programs in effect as of the date of the report, including—

(A) the extent to which the programs are being carried out in accordance with this Act; and

(B) the status of funding requests and appropriations for those programs;

(2) identifies within the planning, budgeting, and construction process all types of Federal facility procedures that inhibit new and existing Federal facilities from becoming high-performance green buildings as measured by—

(A) a silver rating, as defined by the Leadership in Energy and Environmental Design Building Rating System standard established by the United States Green Building Council (or an equivalent rating obtained through a comparable system); or

(B) an improved or higher rating standard, as identified by the Committee;

(3) identifies inconsistencies, as reported to the Committee, in Federal law with respect to product acquisition guidelines and high-performance product guidelines;

(4) recommends language for uniform standards for use by Federal agencies in environmentally responsible acquisition;

(5) in coordination with the Office of Management and Budget, reviews the budget process for capital programs with respect to alternatives for—

(A) restructuring of budgets to require the use of complete energy- and environmental-cost accounting;

(B) using operations expenditures in budget-related decisions while simultaneously incorporating productivity and health measures (as those measures can be quantified by the Office, with the assistance of universities and national laboratories);

(C) permitting Federal agencies to retain all identified savings accrued as a result of the use of life cycle costing; and

(D) identifying short- and long-term cost savings that accrue from high-performance green buildings, including those relating to health and productivity;

(6) identifies green, self-sustaining technologies to address the operational needs of Federal facilities in times of national security emergencies, natural disasters, or other dire emergencies;

(7) summarizes and highlights development, at the State and local level, of green

building initiatives, including Executive orders, policies, or laws adopted promoting green building (including the status of implementation of those initiatives); and

(8) includes, for the 2-year period covered by the report, recommendations to address each of the matters, and a plan for implementation of each recommendation, described in paragraphs (1) through (6).

(d) **IMPLEMENTATION.**—The Office shall carry out each plan for implementation of recommendations under subsection (c)(7).

#### **SEC. 103. GREEN BUILDING ADVISORY COMMITTEE.**

(a) **ESTABLISHMENT.**—Not later than 180 days after the date of enactment of this Act, the Director shall establish an advisory committee, to be known as the “Green Building Advisory Committee”.

(b) **MEMBERSHIP.**—

(1) **IN GENERAL.**—The Committee shall be composed of representatives of, at a minimum—

(A) each agency referred to in section 102(b)(1); and

(B) other relevant agencies and entities, as determined by the Director, including at least 1 representative of each of—

(i) State and local governmental green building programs;

(ii) independent green building associations or councils;

(iii) building experts, including architects, material suppliers, and construction contractors;

(iv) security advisors focusing on national security needs, natural disasters, and other dire emergency situations; and

(v) environmental health experts, including those with experience in children's health.

(2) **NON-FEDERAL MEMBERS.**—The total number of non-Federal members on the Committee at any time shall not exceed 15.

(c) **MEETINGS.**—The Director shall establish a regular schedule of meetings for the Committee.

(d) **DUTIES.**—The Committee shall provide advice and expertise for use by the Director in carrying out the duties under this Act, including such recommendations relating to Federal activities carried out under sections 104 through 106 as are agreed to by a majority of the members of the Committee.

(e) **FACA EXEMPTION.**—The Committee shall not be subject to section 14 of the Federal Advisory Committee Act (5 U.S.C. App.).

#### **SEC. 104. PUBLIC OUTREACH.**

The Director, in coordination with the Committee, shall carry out public outreach to inform individuals and entities of the information and services available Government-wide by—

(1) establishing and maintaining a national high-performance green building clearinghouse, including on the Internet, that—

(A) identifies existing similar efforts and coordinates activities of common interest; and

(B) provides information relating to high-performance green buildings, including hyperlinks to Internet sites that describe related activities, information, and resources of—

(i) the Federal Government;

(ii) State and local governments;

(iii) the private sector (including non-governmental and nonprofit entities and organizations); and

(iv) other relevant organizations, including those from other countries;

(2) identifying and recommending educational resources for implementing high-performance green building practices, including security and emergency benefits and practices;

(3) providing access to technical assistance on using tools and resources to make more

cost-effective, energy-efficient, health-protective, and environmentally beneficial decisions for constructing high-performance green buildings, including tools available to conduct life-cycle costing and life-cycle assessment;

(4) providing information on application processes for certifying a high-performance green building, including certification and commissioning;

(5) providing technical information, market research, or other forms of assistance or advice that would be useful in planning and constructing high-performance green buildings; and

(6) using such other methods as are determined by the Director to be appropriate.

#### **SEC. 105. RESEARCH AND DEVELOPMENT.**

(a) **ESTABLISHMENT.**—The Director, in coordination with the Committee, shall—

(1)(A) survey existing research and studies relating to high-performance green buildings; and

(B) coordinate activities of common interest;

(2) develop and recommend a high-performance green building research plan that—

(A) identifies information and research needs, including the relationships between human health, occupant productivity, and each of—

(i) emissions from materials and products in the building;

(ii) natural day lighting;

(iii) ventilation choices and technologies;

(iv) heating, cooling, and system control choices and technologies;

(v) moisture control and mold;

(vi) maintenance, cleaning, and pest control activities;

(vii) acoustics; and

(viii) other issues relating to the health, comfort, productivity, and performance of occupants of the building; and

(B) promotes the development and dissemination of high-performance green building measurement tools that, at a minimum, may be used—

(i) to monitor and assess the life-cycle performance of facilities (including demonstration projects) built as high-performance green buildings; and

(ii) to perform life-cycle assessments;

(3) assist the budget and life-cycle costing functions of the Office under section 106;

(4) study and identify potential benefits of green buildings relating to security, natural disaster, and emergency needs of the Federal Government; and

(5) support other research initiatives determined by the Office.

(b) **INDOOR AIR QUALITY.**—The Director, in consultation with the Committee, shall develop and carry out a comprehensive indoor air quality program for all Federal facilities to ensure the safety of Federal workers and facility occupants—

(1) during new construction and renovation of facilities; and

(2) in existing facilities.

#### **SEC. 106. BUDGET AND LIFE-CYCLE COSTING AND CONTRACTING.**

(a) **ESTABLISHMENT.**—The Director, in coordination with the Committee, shall—

(1) identify, review, and analyze current budget and contracting practices that affect achievement of high-performance green buildings, including the identification of barriers to green building life-cycle costing and budgetary issues;

(2) develop guidance and conduct training sessions with budget specialists and contracting personnel from Federal agencies and budget examiners to apply life-cycle cost criteria to actual projects;

(3) identify tools to aid life-cycle cost decisionmaking; and

(4) explore the feasibility of incorporating the benefits of green buildings, such as security benefits, into a cost-budget analysis to aid in life-cycle costing for budget and decision making processes.

#### SEC. 107. AUTHORIZATION OF APPROPRIATIONS.

There is authorized to be appropriated to carry out this title \$4,000,000 for each of fiscal years 2008 through 2012, to remain available until expended.

### TITLE II—HEALTHY HIGH-PERFORMANCE SCHOOLS

#### SEC. 201. DEFINITION OF HIGH-PERFORMANCE SCHOOL.

In this title, the term “high-performance school” has the meaning given the term “healthy, high-performance school building” in section 5586 of the Elementary and Secondary Education Act of 1965 (20 U.S.C. 7277e).

#### SEC. 202. GRANTS FOR HEALTHY SCHOOL ENVIRONMENTS.

The Administrator of the Environmental Protection Agency, in consultation with the Secretary of Education, may provide grants to qualified State agencies for use in—

- (1) providing technical assistance for programs of the Environmental Protection Agency (including the Tools for Schools Program and the Healthy School Environmental Assessment Tool) to schools for use in addressing environmental issues; and
- (2) development of State school environmental quality plans that include—
  - (A) standards for school building design, construction, and renovation; and
  - (B) identification of ongoing school building environmental problems in the State and recommended solutions to address those problems, including assessment of information on the exposure of children to environmental hazards in school facilities.

#### SEC. 203. MODEL GUIDELINES FOR SITING OF SCHOOL FACILITIES.

The Administrator of the Environmental Protection Agency, in consultation with the Secretary of Education and the Secretary of Health and Human Services, shall develop school site selection guidelines that account for—

- (1) the special vulnerability of children to hazardous substances or pollution exposures in any case in which the potential for contamination at a potential school site exists;
- (2) modes of transportation available to students and staff; and
- (3) the potential use of a school at the site as an emergency shelter.

#### SEC. 204. PUBLIC OUTREACH.

(a) IN GENERAL.—The Administrator of the Environmental Protection Agency shall provide to the Director information relating to all activities carried out under this title, which the Director shall include in the report described in section 102(c).

(b) PUBLIC OUTREACH.—The Director shall ensure, to the maximum extent practicable, that the public clearinghouse established under section 104 receives and makes available information on the exposure of children to environmental hazards in school facilities, as provided by the Administrator of the Environmental Protection Agency.

#### SEC. 205. ENVIRONMENTAL HEALTH PROGRAM.

(a) IN GENERAL.—The Administrator of the Environmental Protection Agency, in consultation with the Secretary of Education, the Secretary of Health and Human Services, and other relevant agencies, shall issue guidelines for use by the State in developing and implementing an environmental health program for schools that—

- (1) takes into account the status and findings of Federal research initiatives established under this Act and other relevant Federal law with respect to school facilities, in-

cluding relevant updates on trends in the field, such as the impact of school facility environments on student and staff—

- (A) health, safety, and productivity; and
- (B) disabilities or special needs;
- (2) provides research using relevant tools identified or developed in accordance with section 105(a) to quantify the relationships between—
  - (A) human health, occupant productivity, and student performance; and
  - (B) with respect to school facilities, each of—
    - (i) pollutant emissions from materials and products;
    - (ii) natural day lighting;
    - (iii) ventilation choices and technologies;
    - (iv) heating and cooling choices and technologies;
    - (v) moisture control and mold;
    - (vi) maintenance, cleaning, and pest control activities;
    - (vii) acoustics; and
    - (viii) other issues relating to the health, comfort, productivity, and performance of occupants of the school facilities;
- (3) provides technical assistance on siting, design, management, and operation of school facilities, including facilities used by students with disabilities or special needs;
- (4) collaborates with federally funded pediatric environmental health centers to assist in on-site school environmental investigations;
- (5) assists States and the public in better understanding and improving the environmental health of children; and
- (6) provides to the Office a biennial report of all activities carried out under this title, which the Director shall include in the report described in section 102(c).

(b) PUBLIC OUTREACH.—The Director shall ensure, to the maximum extent practicable, that the public clearinghouse established under section 104 receives and makes available—

- (1) information from the Administrator of the Environmental Protection Agency that is contained in the report described in subsection (a)(6); and
- (2) information on the exposure of children to environmental hazards in school facilities, as provided by the Administrator of the Environmental Protection Agency.

There is authorized to be appropriated to carry out this title \$10,000,000 for the period of fiscal years 2008 through 2012, to remain available until expended.

### TITLE III—STRENGTHENING FEDERAL LEADERSHIP

#### SEC. 206. AUTHORIZATION OF APPROPRIATIONS.

There is authorized to be appropriated to carry out this title \$10,000,000 for the period of fiscal years 2008 through 2012, to remain available until expended.

### TITLE III—STRENGTHENING FEDERAL LEADERSHIP

#### SEC. 301. INCENTIVES.

As soon as practicable after the date of enactment of this Act, the Director shall identify incentives to encourage the use of green buildings and related technology in the operations of the Federal Government, including through—

- (1) the provision of recognition awards; and
- (2) the maximum feasible retention of financial savings in the annual budgets of Federal agencies.

#### SEC. 302. FEDERAL PROCUREMENT.

(a) IN GENERAL.—Not later than 2 years after the date of enactment of this Act, the Director of the Office of Federal Procurement Policy, in consultation with the Director and the Under Secretary of Defense for Acquisition, Technology, and Logistics, shall promulgate revisions of the applicable acquisition regulations, to take effect as of the date of promulgation of the revisions—

- (1) to direct any Federal procurement executives involved in the acquisition, construction, or major renovation (including contracting for the construction or major renovation) of any facility, to the maximum extent practicable—

- (A) to employ integrated design principles;
- (B) to optimize building and systems energy performance;
- (C) to protect and conserve water;
- (D) to enhance indoor environmental quality; and
- (E) to reduce environmental impacts of materials and waste flows; and

(2) to direct Federal procurement executives involved in leasing buildings, to give preference to the lease of facilities that, to the maximum extent practicable—

- (A) are energy-efficient; and
- (B) have applied contemporary high-performance and sustainable design principles during construction or renovation.

(b) GUIDANCE.—Not later than 90 days after the date of promulgation of the revised regulations under subsection (a), the Director shall issue guidance to all Federal procurement executives providing direction and the option to renegotiate the design of proposed facilities, renovations for existing facilities, and leased facilities to incorporate improvements that are consistent with this section.

#### SEC. 303. FEDERAL GREEN BUILDING PERFORMANCE.

(a) IN GENERAL.—Not later than October 31 of each of the 2 fiscal years following the fiscal year in which this Act is enacted, and at such times thereafter as the Comptroller General of the United States determines to be appropriate, the Comptroller General of the United States shall, with respect to the fiscal years that have passed since the preceding report—

- (1) conduct an audit of the implementation of this Act; and
- (2) submit to the Office, the Committee, the Administrator, and Congress a report describing the results of the audit.

(b) CONTENTS.—An audit under subsection (a) shall include a review, with respect to the period covered by the report under subsection (a)(2), of—

- (1) budget, life-cycle costing, and contracting issues, using best practices identified by the Comptroller General of the United States and heads of other agencies in accordance with section 106;
- (2) the level of coordination among the Office, the Office of Management and Budget, and relevant agencies;
- (3) the performance of the Office in carrying out the implementation plan;
- (4) the design stage of high-performance green building measures;
- (5) high-performance building data that were collected and reported to the Office; and
- (6) such other matters as the Comptroller General of the United States determines to be appropriate.

(c) ENVIRONMENTAL STEWARDSHIP SCORECARD.—The Director shall consult with the Committee to enhance, and assist in the implementation of, the Environmental Stewardship Scorecard announced at the White House summit on Federal sustainable buildings in January 2006, to measure the implementation by each Federal agency of sustainable design and green building initiatives.

### TITLE IV—DEMONSTRATION PROJECT

#### SEC. 401. COORDINATION OF GOALS.

(a) IN GENERAL.—The Director shall establish guidelines to implement a demonstration project to contribute to the research goals of the Office.

#### (b) PROJECTS.—

(1) IN GENERAL.—In accordance with guidelines established by the Director under subsection (a) and the duties of the Director described in title I, the Director shall carry out 3 demonstration projects.



(2) LOCATION OF PROJECTS.—Each project carried out under paragraph (1) shall be located in a Federal building in a State recommended by the Director in accordance with subsection (c).

(3) REQUIREMENTS.—Each project carried out under paragraph (1) shall—

(A) provide for the evaluation of the information obtained through the conduct of projects and activities under this Act; and

(B) achieve a platinum rating, as defined by the Leadership in Energy and Environmental Design Building Rating System standard established by the United States Green Building Council (or an equivalent rating obtained through a comparable system).

(c) CRITERIA.—With respect to the existing or proposed Federal facility at which a demonstration project under this section is conducted, the Federal facility shall—

(1) be an appropriate model for a project relating to—

(A) the effectiveness of high-performance technologies;

(B) analysis of materials, components, and systems, including the impact on the health of building occupants;

(C) life-cycle costing and life-cycle assessment of building materials and systems; and

(D) location and design that promote access to the Federal facility through walking, biking, and mass transit; and

(2) possess sufficient technological and organizational adaptability.

(d) REPORT.—Not later than 1 year after the date of enactment of this Act, and annually thereafter through September 30, 2013, the Director shall submit to the Administrator a report that describes the status of and findings regarding the demonstration project.

#### SEC. 402. AUTHORIZATION OF APPROPRIATIONS.

There is authorized to be appropriated to carry out the Federal demonstration project described in section 401(b) \$10,000,000 for the period of fiscal years 2008 through 2012, to remain available until expended.

By Mr. CONRAD (for himself, Ms. COLLINS, Ms. CANTWELL, and Mr. DURBIN):

S. 507. A bill to amend title XVIII of the Social Security Act to provide for reimbursement of certified midwife services and to provide for more equitable reimbursement rates for certified nurse-midwife services; to the Committee on Finance.

Mr. CONRAD. Mr. President, today I am introducing the Midwifery Care Access and Reimbursement Equity (M-CARE) Act of 2007. For too many years, certified nurse midwives (CNMs) have not received adequate reimbursement under the Medicare program. My legislation takes steps to improve reimbursement for these important healthcare providers.

Since 1988, CNMs have been authorized to provide maternity-related services to Medicare-eligible women of child-bearing age. There are approximately three million disabled women of child-bearing age on Medicare; however, if they choose to utilize a CNM for “well women” services, the CNM is only reimbursed at 65 percent of the physician fee schedule. This is not right and does not come close to offsetting the costs incurred by these professionals.

At this incredibly low rate of reimbursement, the Medicare Payment Ad-

visory Committee (MedPAC) agrees that a CNM simply cannot afford to provide services to Medicare patients and has supported increasing reimbursement for CNMs. In fact, the Commission recommended in 2002 that CNMs’ reimbursement be increased and acknowledged that the care provided by these individuals is at least comparable to similar providers.

My legislation would make several changes to improve the ability of CNMs and certified midwives (CMs) to effectively serve the Medicare-eligible population. First, and most importantly, my bill recognizes the need to increase Medicare reimbursement for CNMs by raising the reimbursement level from 65 percent to 100 percent of the physician fee schedule. CNMs provide the same care as physicians; therefore, it is only fair to reimburse CNMs at the same level. Several states have recognized this in their Medicaid programs—approximately 29 States reimburse at 100 percent of the physician fee schedule for out-of-hospital services.

In addition, the M-CARE Act would establish recognition for a certified midwife (CM) to provide services under Medicare. Despite the fact that CNMs and CMs provide the same services, Medicare has yet to recognize CMs as eligible providers. My bill would change this.

This bill will enhance access to “well woman” care for thousands of women in underserved communities and make several needed changes to improve access to midwives. I urge my colleagues to support this legislation.

By Mr. GRASSLEY:

S. 508. A bill to amend the Congressional Accountability Act of 1995 to apply whistleblower protections available to certain executive branch employees to legislative branch employees, and for other purposes; to the Committee on Homeland Security and Governmental Affairs.

Mr. GRASSLEY. Mr. President, I rise to reintroduce the Congressional Whistleblower Protection Act of 2007, which will extend whistleblower protections currently available to certain executive branch employees to legislative branch employees.

Presently, executive branch employees are shielded from retaliation for exposing waste, fraud, or abuse by the Whistleblower Protection Act. The bill I’m introducing today simply extends those same protections to legislative branch employees.

A theme that has dominated this new Congress, as well as the elections this past November, is accountability and responsibility in Washington. I have fought hard for whistleblowers over the years because they are key in our efforts to ensure government accountability to the people we are sent here to serve. In most instances, the only reason we discover waste or fraud is because employees are brave enough to stand up to the wrongdoers and expose their offenses. Without these whistle-

blowers, the American taxpayer would continue to foot the bill.

The Office of Compliance has called for these changes on numerous occasions in recent years, and they are very supportive of this bill. We have already taken the steps to protect whistleblowers in the executive branch. It doesn’t make sense not to extend these same protections to whistleblowers in our own backyard. My bill will, very simply, give congressional employees the same protections that workers in the other branches of government already possess.

I hope my colleagues will join me in supporting this bill to ensure that those who help us in the fight to hold government accountable are not punished for their efforts.

I ask unanimous consent that the text of this bill be printed in the RECORD.

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

S. 508

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

#### SECTION 1. APPLICATION OF WHISTLEBLOWER PROTECTION RULES TO LEGISLATIVE BRANCH EMPLOYEES.

(a) SHORT TITLE.—This Act may be cited as the “Congressional Whistleblower Protection Act of 2007”.

(b) IN GENERAL.—Part A of title II of the Congressional Accountability Act of 1995 (2 U.S.C. 1311 et seq.) is amended—

(1) in the heading, by striking “fair labor standards,” and all that follows and inserting “and other protections and benefits”;

(2) by redesignating section 207 as section 208; and

(3) by inserting after section 206 the following:

#### “SEC. 207. RIGHTS AND PROTECTIONS UNDER WHISTLEBLOWER PROTECTION RULES.

“(a) RIGHTS AND PROTECTIONS DESCRIBED.—

“(1) IN GENERAL.—No employing office may take or fail to take, or threaten to take or fail to take, a personnel action (within the meaning of chapter 23 of title 5, United States Code) with respect to any covered employee or applicant for employment because of—

“(A) any disclosure of information by a covered employee or applicant which the employee or applicant reasonably believes evidences—

“(i) a violation of any law, rule, or regulation; or

“(ii) gross mismanagement, a gross waste of funds, an abuse of authority, or a substantial and specific danger to public health or safety;

if such disclosure is not specifically prohibited by law and if such information is not specifically required by Executive order or the rules of the Senate or the House of Representatives to be kept secret in the interest of national defense or the conduct of foreign affairs; or

“(B) any disclosure to the General Counsel, or to the Inspector General of a legislative or executive agency or another employee designated by the head of the legislative or executive agency to receive such disclosures, of information which the employee or applicant reasonably believes evidences—

“(i) a violation of any law, rule, or regulation; or

“(ii) gross mismanagement, a gross waste of funds, an abuse of authority, or a substantial and specific danger to public health or safety.

“(2) DEFINITIONS.—For purposes of this section and for purposes of applying the procedures established under title IV for the consideration of alleged violations of this section—

“(A) the term ‘covered employee’ includes an employee of the Government Accountability Office or Library of Congress; and

“(B) the term ‘employing office’ includes the Government Accountability Office and the Library of Congress.

“(b) REMEDY.—The remedy for a violation of subsection (a) shall be such remedy as would be appropriate if awarded under chapter 12 of title 5, United States Code, with respect to a prohibited personnel practice described in section 2302(b)(8) of such title.

“(C) REGULATIONS TO IMPLEMENT SECTION.—

“(1) IN GENERAL.—The Board shall, pursuant to section 304, issue regulations to implement this section.

“(2) AGENCY REGULATIONS.—The regulations issued under paragraph (1) shall be the same as the substantive regulations promulgated by the Merit Systems Protection Board to implement chapters 12 and 23 of title 5, United States Code, except to the extent that the Board of Directors of the Office of Compliance may determine, for good cause shown and stated together with the regulation, that a modification of such regulations would be more effective for the implementation of the rights and protections under this section.”

(C) TECHNICAL AND CONFORMING AMENDMENTS.—

(1) TABLE OF CONTENTS.—The table of contents for part A of title II of the Congressional Accountability Act of 1995 is amended—

(A) in the item relating to part A, by striking “**FAIR LABOR STANDARDS**,” and all that follows and inserting “**AND OTHER PROTECTIONS AND BENEFITS**”;

(B) by redesignating the item relating to section 207 as relating to section 208; and

(C) by inserting after the item relating to section 206 the following:

“Sec. 207. Rights and protections under whistleblower protection rules.”

(2) APPLICATION OF LAWS.—Section 102(a) of the Congressional Accountability Act of 1995 (2 U.S.C. 1302(a)) is amended by adding at the end the following:

“(12) Section 2302(b)(8) of title 5, United States Code.”

Mr. INOUE (for himself, Mr. STEVENS, Mr. ROCKEFELLER, Mr. LOTT, and Mr. LAUTENBERG):

S. 509. A bill to provide improved aviation security, and for other purposes; to the Committee on Commerce, Science, and Transportation.

Mr. INOUE. Mr. President, I rise today to introduce the Aviation Security Improvement Act with Senators STEVENS, ROCKEFELLER, LOTT, and LAUTENBERG, who are all original co-sponsors of this legislation.

When the 9/11 Commission released its report in 2004, the Commission expressed continuing concern over the state of air cargo security, the screening of passengers and baggage, access controls at airports, and the security of general aviation. Congress responded then and enacted measures to address inefficiencies highlighted by the Com-

mission. However, implementation through the rulemaking process was slow, and as a result, significant shortfalls in our security regime remain.

In fact, a little more than year ago, the 9/11 Public Discourse project issued a scorecard that gave inadequate grades in those key areas where the Commission had advocated for improvements in aviation security. Checked Baggage and Cargo Screening received a “D,” Airline Passenger Explosive Screening received a “C,” and Airline Passenger Prescreening received an “F.”

Over the past year, the Transportation Security Administration, TSA, has continued working to significantly bolster air cargo security in the United States. While that is a good step in response to the report card, more must be done. The government must remain vigilant in its effort to provide security for our Nation, and the steps proposed in this bill will both improve our existing security system and give TSA the flexibility to combat new and emerging threats.

The bill we are introducing today would require the screening of all cargo going on passenger aircraft within 3 years. We expect TSA to develop a robust screening program that improves upon current measures and ensures the security of all cargo transported in commercial passenger air carriers.

To improve our ability to detect explosives in checked baggage and at passenger screening checkpoints, the bill extends the Aviation Security Capital Fund and promotes the purchase and installation of advanced baggage screening systems that can be integrated into the daily workings of our Nation’s air transportation system. This capital investment will improve security screening by permitting TSA employees to better focus on potential threats while reducing the high workplace injury rates.

The bill addresses airline passenger explosive screening in several ways:

1. By promoting advanced research and development for checkpoint technology;

2. By enhancing screener training to more clearly identify and address potential threats; and

3. By requiring the Administration to complete and implement a plan over the next year that thoroughly addresses the threat of and response to carry-on explosives.

Airline passenger prescreening also remains a primary concern of the Congress. Not enough progress has been made by the TSA to develop an advanced passenger prescreening system since it took on this task nearly 4 years ago. Too many passengers are inconvenienced each year by false positives when matched against passenger watchlists.

Our bill would ensure a system is in place to coordinate passenger redress matters, and that the TSA moves rapidly to develop a strategic plan to test and implement an advanced passenger prescreening system.

Our bill also takes steps to improve general aviation security, airport access issues for airline employees, screener staffing issues, and other issues where there have been consistent shortcomings over the past several years.

The 9/11 Commission’s report and subsequent Public Discourse project helped keep Congress and the Administration focused on the need for aviation security. While they did not have all the answers for quick fixes, they did offer a vital blueprint, particularly in the areas of infrastructure and transportation system security.

My colleagues and I used that guideline in drafting the legislation we are introducing today. We believe that once this bill is enacted, it will significantly improve aviation security in the specific areas I have highlighted, and the aviation system as a whole. I look forward to working with my colleagues to move this bill quickly. We have had 5 years to consider what does and does not work. Now it is time to implement what we have learned.

I ask unanimous consent that this bill be printed in the RECORD.

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

S. 509

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

#### SEC. 1. SHORT TITLE; TABLE OF CONTENTS.

(a) SHORT TITLE.—This Act may be cited as the “Aviation Security Improvement Act”.

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

#### TITLE —AVIATION SECURITY

- Sec. 1. Short title; table of contents.
- Sec. 2. Extension of authorization for aviation security funding.
- Sec. 3. Passenger aircraft cargo screening.
- Sec. 4. Blast-resistant cargo containers.
- Sec. 5. Protection of air cargo on passenger planes from explosives.
- Sec. 6. In-line baggage screening.
- Sec. 7. Enhancement of in-line baggage system deployment.
- Sec. 8. Research and development of aviation transportation security technology.
- Sec. 9. Certain TSA personnel limitations not to apply.
- Sec. 10. Specialized training.
- Sec. 11. Explosive detection at passenger screening checkpoints.
- Sec. 12. Appeal and redress process for passengers wrongly delayed or prohibited from boarding a flight.
- Sec. 13. Repair station security.
- Sec. 14. Strategic plan to test and implement advanced passenger prescreening system.
- Sec. 15. General aviation security.
- Sec. 16. Security credentials for airline crews.

#### SEC. 2. EXTENSION OF AUTHORIZATION FOR AVIATION SECURITY FUNDING.

Section 48301(a) of title 49, United States Code, is amended by striking “and 2006” and inserting “2006, 2007, 2008, and 2009”.

#### SEC. 3. PASSENGER AIRCRAFT CARGO SCREENING.

(a) IN GENERAL.—Section 44901 of title 49, United States Code, is amended—

(1) by redesignating subsections (g) and (h) as subsections (h) and (i), respectively; and

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

“(g) AIR CARGO ON PASSENGER AIRCRAFT.—

“(1) IN GENERAL.—Not later than 3 years after the date of enactment of the Aviation Security Improvement Act, the Secretary of Homeland Security, acting through the Administrator of the Transportation Security Administration, shall establish a system to screen all cargo transported on passenger aircraft operated by an air carrier or foreign air carrier in air transportation or intrastate air transportation to ensure the security of all such passenger aircraft carrying cargo.

“(2) MINIMUM STANDARDS.—The system referred to in paragraph (1) shall require, at a minimum, that the equipment, technology, procedures, personnel, or other methods determined by the Administrator of the Transportation Security Administration, provide a level of security comparable to the level of security in effect for passenger checked baggage.

“(3) REGULATIONS.—

“(A) INTERIM FINAL RULE.—The Secretary of Homeland Security may issue an interim final rule as a temporary regulation to implement this subsection without regard to the provisions of chapter 5 of title 5.

“(B) FINAL RULE.—

“(i) IN GENERAL.—If the Secretary issues an interim final rule under subparagraph (A), the Secretary shall issue, not later than 1 year after the effective date of the interim final rule, a final rule as a permanent regulation to implement this subsection in accordance with the provisions of chapter 5 of title 5.

“(ii) FAILURE TO ACT.—If the Secretary does not issue a final rule in accordance with clause (i) on or before the last day of the 1-year period referred to in clause (i), the Secretary shall submit a report to the Congress explaining why the final rule was not timely issued and providing an estimate of the earliest date on which the final rule will be issued. The Secretary shall submit the first such report within 10 days after such last day and submit a report to the Congress containing updated information every 60 days thereafter until the final rule is issued.

“(iii) SUPERSEDING OF INTERIM FINAL RULE.—The final rule issued in accordance with this subparagraph shall supersede the interim final rule issued under subparagraph (A).

“(4) REPORT.—Not later than 1 year after the date on which the system required by paragraph (1) is established, the Secretary shall transmit a report to Congress that details and explains the system.”

(b) ASSESSMENT OF EXEMPTIONS.—

(1) TSA ASSESSMENT OF EXEMPTIONS.—

(A) IN GENERAL.—Not later than 180 days after the date of enactment of this Act, the Secretary of Homeland Security, through the Administrator of the Transportation Security Administration, shall submit a report to Congress and to the Comptroller General containing an assessment of each exemption granted under section 44901(i) of title 49, United States Code, for the screening required by section 44901(g)(1) of that title for cargo transported on passenger aircraft and an analysis to assess the risk of maintaining such exemption. The Secretary may submit the report in both classified and redacted formats if the Secretary determines that such action is appropriate or necessary.

(B) CONTENTS.—The report shall include—

(i) the rationale for each exemption;

(ii) a statement of the percentage of cargo that is not screened as a result of each exemption;

(iii) the impact of each exemption on aviation security;

(iv) the projected impact on the flow of commerce of eliminating such exemption;

(v) a statement of any plans, and the rationale, for maintaining, changing, or eliminating each exemption.

(2) GAO ASSESSMENT.—Not later than 120 days after the date on which the report required under paragraph (1) is submitted, the Comptroller General shall review the report and provide to Congress an assessment of the methodology used for determinations made by the Secretary for maintaining, changing, or eliminating an exemption.

#### SEC. 4. BLAST-RESISTANT CARGO CONTAINERS.

Section 44901 of title 49, United States Code, is amended by adding at the end thereof the following:

“(i) BLAST-RESISTANT CARGO CONTAINERS.—

“(1) IN GENERAL.—Before January 1, 2008, the Administrator of the Transportation Security Administration shall—

“(A) evaluate the results of the blast-resistant cargo container pilot program instituted before the date of enactment of the Aviation Security Improvement Act;

“(B) based on that evaluation, begin the acquisition of a sufficient number of blast-resistant cargo containers to meet the requirements of the Transportation Security Administration's cargo security program under paragraph (2); and

“(C) develop a system under which the Administrator—

“(i) will make such containers available for use by passenger aircraft operated by air carriers or foreign air carriers in air transportation or intrastate air transportation on a random or risk-assessment basis as determined by the Administrator, in sufficient number to enable the carriers to meet the requirements of the Administration's cargo security system; and

“(ii) provide for the storage, maintenance, and distribution of such containers.

“(2) DISTRIBUTION TO AIR CARRIERS.—Within 90 days after the date on which the Administrator completes development of the system required by paragraph (1)(C), the Administrator of the Transportation Security Administration shall implement that system and begin making blast-resistant cargo containers available to such carriers as necessary.”

#### SEC. 5. PROTECTION OF AIR CARGO ON PASSENGER PLANES FROM EXPLOSIVES.

(a) TECHNOLOGY RESEARCH AND PILOT PROJECTS.—

(1) RESEARCH AND DEVELOPMENT.—The Secretary of Homeland Security shall expedite research and development for technology that can disrupt or prevent an explosive device from being introduced onto a passenger plane or from damaging a passenger plane while in flight or on the ground. The research shall include blast resistant cargo containers and other promising technology and will be used in concert with implementation of section 4 of this Act.

(2) PILOT PROJECTS.—The Secretary, in conjunction with the Secretary of Transportation, shall establish a grant program to fund pilot projects—

(A) to deploy technologies described in paragraph (1); and

(B) to test technology to expedite the recovery, development, and analysis of information from aircraft accidents to determine the cause of the accident, including deployable flight deck and voice recorders and remote location recording devices.

(b) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be appropriated to the Secretary of Homeland Security for fiscal year 2008 such sums as may be necessary to carry out this section, such funds to remain available until expended.

#### SEC. 6. IN-LINE BAGGAGE SCREENING.

(a) EXTENSION OF AUTHORIZATION.—Section 44923(i)(1) of title 49, United States Code, is

amended by striking “2007.” and inserting “2007, and \$450,000,000 for each of fiscal years 2008 and 2009.”

(b) REPORT.—Within 30 days after the date of enactment of this Act, the Secretary of Homeland Security shall submit the report the Secretary was required by section 4019(d) of the Intelligence Reform and Terrorism Prevention Act of 2004 (49 U.S.C. 44901 note) to have submitted in conjunction with the submission of the budget for fiscal year 2006.

#### SEC. 7. ENHANCEMENT OF IN-LINE BAGGAGE SYSTEM DEPLOYMENT.

(a) IN GENERAL.—Section 44923 of title 49, United States Code, is amended—

(1) by striking “may” in subsection (a) and inserting “shall”;

(2) by striking “may” in subsection (d)(1) and inserting “shall”;

(3) by striking “2007” in subsection (h)(1) and inserting “2028”;

(4) by striking paragraphs (2) and (3) of subsection (h) and inserting the following:

“(2) ALLOCATION.—Of the amount made available under paragraph (1) for a fiscal year, not less than \$200,000,000 shall be allocated to fulfill letters of intent issued under subsection (d).

“(3) DISCRETIONARY GRANTS.—Of the amount made available under paragraph (1) for a fiscal year, up to \$50,000,000 shall be used to make discretionary grants, with priority given to small hub airports and non-hub airports.”; and

(5) by redesignating subsection (i) as subsection (j) and inserting after subsection (h) the following:

“(i) LEVERAGED FUNDING.—For purposes of this section, a grant under subsection (a) to an airport sponsor to service an obligation issued by or on behalf of that sponsor to fund a project described in subsection (a) shall be considered to be a grant for that project.”

(b) PRIORITIZATION OF PROJECTS.—

(1) IN GENERAL.—The Administrator shall create a prioritization schedule for airport security improvement projects described in section 44923(b) of title 49, United States Code, based on risk and other relevant factors, to be funded under the grant program provided by that section. The schedule shall include both hub airports (as defined in section 41731(a)(3) of title 49, United States Code) and nonhub airports (as defined in section 41731(a)(4) of title 49, United States Code).

(2) AIRPORTS THAT HAVE COMMENCED PROJECTS.—The schedule shall include airports that have incurred eligible costs associated with development of partial in-line baggage systems before the date of enactment of this Act in reasonable anticipation of receiving a grant under section 44923 of title 49, United States Code, in reimbursement of those costs but that have not received such a grant.

(3) REPORT.—Within 180 days after the date of enactment of this Act, the Administrator shall provide a copy of the prioritization schedule, a corresponding timeline, and a description of the funding allocation under section 44923 of title 49, United States Code, to the Senate Committee on Commerce, Science, and Transportation and the House of Representatives Committee on Homeland Security.

#### SEC. 8. RESEARCH AND DEVELOPMENT OF AVIATION TRANSPORTATION SECURITY TECHNOLOGY.

Section 137(a) of the Aviation and Transportation Security Act (49 U.S.C. 44912 note) is amended—

(1) by striking “2002 through 2006,” and inserting “2006 through 2009,”;

(2) by striking “aviation” and inserting “transportation”; and

(3) by striking “2002 and 2003” and inserting “2006 through 2009”.

**SEC. 9. CERTAIN TSA PERSONNEL LIMITATIONS NOT TO APPLY.**

(a) IN GENERAL.—Notwithstanding any provision of law to the contrary, any statutory limitation on the number of employees in the Transportation Security Administration, before or after its transfer to the Department of Homeland Security from the Department of Transportation, does not apply after fiscal year 2007.

(b) AVIATION SECURITY.—Notwithstanding any provision of law imposing a limitation on the recruiting or hiring of personnel into the Transportation Security Administration to a maximum number of permanent positions, the Secretary of Homeland Security shall recruit and hire such personnel into the Administration as may be necessary—

(1) to provide appropriate levels of aviation security; and

(2) to accomplish that goal in such a manner that the average aviation security-related delay experienced by airline passengers is reduced to a level of less than 10 minutes.

**SEC. 10. SPECIALIZED TRAINING.**

The Administrator of the Transportation Security Administration shall provide advanced training to transportation security officers for the development of specialized security skills, including behavior observation and analysis, explosives detection, and document examination, in order to enhance the effectiveness of layered transportation security measures.

**SEC. 11. EXPLOSIVE DETECTION AT PASSENGER SCREENING CHECKPOINTS.**

(a) IN GENERAL.—Within 90 days after the date of enactment of this Act, the Secretary of Homeland Security shall issue the strategic plan the Secretary was required by section 44925(a) of title 49, United States Code, to have issued within 90 days after the date of enactment of the Intelligence Reform and Terrorism Prevention Act of 2004.

(b) DEPLOYMENT.—Section 44925(b) of title 49, United States Code, is amended by adding at the end thereof the following:

“(3) FULL DEPLOYMENT.—The Secretary shall fully implement the strategic plan within 1 year after the date of enactment of the Aviation Security Improvement Act.”.

**SEC. 12. APPEAL AND REDRESS PROCESS FOR PASSENGERS WRONGLY DELAYED OR PROHIBITED FROM BOARDING A FLIGHT.**

(a) IN GENERAL.—Subtitle C of title IV of the Homeland Security Act of 2002 (6 U.S.C. 231 et seq.) is amended by adding at the end the following:

**“SEC. 431. APPEAL AND REDRESS PROCESS FOR PASSENGERS WRONGLY DELAYED OR PROHIBITED FROM BOARDING A FLIGHT.**

“(a) IN GENERAL.—The Secretary shall establish a timely and fair process for individuals who believe they have been delayed or prohibited from boarding a commercial aircraft because they were wrongly identified as a threat under the regimes utilized by the Transportation Security Administration, the Bureau of Customs and Border Protection, or any other Department entity.

“(b) OFFICE OF APPEALS AND REDRESS.—

“(1) ESTABLISHMENT.—The Secretary shall establish an Office of Appeals and Redress to oversee the process established by the Secretary pursuant to subsection (a).

“(2) RECORDS.—The process established by the Secretary pursuant to subsection (a) shall include the establishment of a method by which the Office of Appeals and Redress, under the direction of the Secretary, will be able to maintain a record of air carrier passengers and other individuals who have been misidentified and have corrected erroneous information.

“(3) INFORMATION.—To prevent repeated delays of an misidentified passenger or other

individual, the Office of Appeals and Redress shall—

“(A) ensure that the records maintained under this subsection contain information determined by the Secretary to authenticate the identity of such a passenger or individual; and

“(B) furnish to the Transportation Security Administration, the Bureau of Customs and Border Protection, or any other appropriate Department entity, upon request, such information as may be necessary to allow such agencies to assist air carriers in improving their administration of the advanced passenger prescreening system and reduce the number of false positives.”.

(b) CLERICAL AMENDMENT.—The table of contents in section 1(b) of such Act is amended by inserting after the item relating to section 430 the following:

“431. Appeal and redress process for passengers wrongly delayed or prohibited from boarding a flight.”.

**SEC. 13. STRATEGIC PLAN TO TEST AND IMPLEMENT ADVANCED PASSENGER PRESCREENING SYSTEM.**

Not later than 180 days after the date of enactment of this Act, the Secretary of Homeland Security, in consultation with the Administrator of the Transportation Security Administration, shall submit to the Congress a plan that—

(1) describes the system to be utilized by the Department of Homeland Security to assume the performance of comparing passenger information, as defined by the Administrator of the Transportation Security Administration, to the automatic selectee and no-fly lists, utilizing appropriate records in the consolidated and integrated terrorist watchlist maintained by the Federal government;

(2) provides a projected timeline for each phase of testing and implementation of the system;

(3) explains how the system will be integrated with the prescreening system for passengers on international flights; and

(4) describes how the system complies with section 552a of title 5, United States Code.

**SEC. 14. REPAIR STATION SECURITY.**

(a) CERTIFICATION OF FOREIGN REPAIR STATIONS SUSPENSION.—If the regulations required by section 44924(f) of title 49, United States Code, are not issued within 90 days after the date of enactment of this Act, the Administrator of the Federal Aviation Administration may not certify any foreign repair station under part 145 of title 14, Code of Federal Regulations, after such 90th day unless the station was previously certified by the Administration under that part.

(b) 6-MONTH DEADLINE FOR SECURITY REVIEW AND AUDIT.—Subsections (a) and (d) of section 44924 of title 49, United States Code, are each amended by striking “18 months” and inserting “6 months”.

**SEC. 15. GENERAL AVIATION SECURITY.**

Section 44901 of title 49, United States Code, is amended by adding at the end thereof the following:

“(i) GENERAL AVIATION AIRPORT SECURITY PROGRAM.—

“(1) IN GENERAL.—Within 1 year after the date of enactment of the Aviation Security Improvement Act the Administrator of the Transportation Security Administration shall—

“(A) develop a standardized threat and vulnerability assessment program for general aviation airports (as defined in section 47135(m)); and

“(B) implement a program to perform such assessments on a risk-assessment basis at general aviation airports.

“(2) GRANT PROGRAM.—Within 6 months after date of enactment of the Aviation Se-

curity Improvement Act the Administrator shall initiate and complete a study of the feasibility of a program, based on a risk-managed approach, to provide grants to general aviation airport operators for projects to upgrade security at general aviation airports (as defined in section 47135(m)). If the Administrator determines that such a program is feasible, the Administrator shall establish such a program.

“(3) APPLICATION TO FOREIGN-REGISTERED GENERAL AVIATION AIRCRAFT.—Within 180 days after the date of enactment of the Aviation Security Improvement Act, the Administrator shall develop a risk-based system under which—

“(A) foreign-registered general aviation aircraft, as identified by the Administrator, in coordination with the Administrator of the Federal Aviation Administration, are required to submit passenger information to the Transportation Security Administration before entering United States airspace; and

“(B) such information is checked against appropriate databases maintained by the Transportation Security Administration.”.

“(4) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be appropriated to the Secretary of Homeland Security such sums as may be necessary to carry out any program established under paragraph (2).”.

**SEC. 16. SECURITY CREDENTIALS FOR AIRLINE CREWS.**

Within 180 days after the date of enactment of this Act, the Administrator of the Transportation Security Administration shall, after consultation with airline, airport, and flight crew representatives, transmit a report to the Senate Committee on Commerce, Science, and Transportation and the House of Representatives Committee on Transportation and Infrastructure on the status of its efforts to institute a sterile area access system or method that will enhance security by properly identifying authorized airline flight deck and cabin crew members at screening checkpoints and granting them expedited access through screening checkpoints. The Administrator shall include in the report recommendations on the feasibility of implementing the system for the domestic aviation industry beginning 1 year after the date on which the report is submitted. The Administrator shall begin full implementation of the system or method not later than 1 year after the date on which the Administrator transmits the report.

**SUBMITTED RESOLUTIONS****SENATE RESOLUTION 72—ACKNOWLEDGING THE SEVERITY OF THE WETLAND LOSS OCCURRING IN LOUISIANA AND SUPPORTING THE OBSERVANCE OF WORLD WETLANDS DAY IN THE UNITED STATES**

Ms. LANDRIEU submitted the following resolution; which was referred to the Committee on Environment and Public Works:

**S. RES. 72**

Whereas Louisiana's coastal wetlands are among the Nation's most diverse and productive ecosystems, home to ospreys, egrets, alligators, shellfish, turtles, sea grasses, and bald cypress trees;

Whereas Louisiana's wetlands are eroding at a rate of 25 square miles per year and, as a result of Hurricane Katrina on August 29, 2005, and Hurricane Rita on September 24, 2005, 217 square miles of wetlands were turned into open water, significantly advancing Louisiana's wetlands loss;