

S. 392

At the request of Mr. REID, the names of the Senator from Nevada (Mr. ENSIGN) and the Senator from Arkansas (Mr. PRYOR) were added as cosponsors of S. 392, a bill to amend title 10, United States Code, to permit retired members of the Armed Forces who have a service-connected disability to receive both military retired pay by reason of their years of military service and disability compensation from the Department of Veterans Affairs for their disability.

S. 423

At the request of Ms. COLLINS, the name of the Senator from Minnesota (Mr. DAYTON) was added as a cosponsor of S. 423, a bill to promote health care coverage parity for individuals participating in legal recreational activities or legal transportation activities.

S. 505

At the request of Mr. HATCH, the name of the Senator from Minnesota (Mr. DAYTON) was added as a cosponsor of S. 505, a bill to amend the Internal Revenue Code of 1986 to encourage and accelerate the nationwide production, retail sale, and consumer use of new motor vehicles that are powered by fuel cell technology, hybrid technology, battery electric technology, alternative fuels, or other advanced motor vehicle technologies, and for other purposes.

S. 537

At the request of Mr. CRAPO, the name of the Senator from Montana (Mr. BURNS) was added as a cosponsor of S. 537, a bill to ensure the availability of spectrum to amateur radio operators.

S. 545

At the request of Ms. SNOWE, the name of the Senator from Mississippi (Mr. LOTT) was added as a cosponsor of S. 545, a bill to amend title I of the Employee Retirement Income Security Act of 1974 to improve access and choice for entrepreneurs with small businesses with respect to medical care for their employees.

S. 547

At the request of Mr. DURBIN, the name of the Senator from New York (Mrs. CLINTON) was added as a cosponsor of S. 547, a bill to encourage energy conservation through bicycling.

S. 569

At the request of Mr. ENSIGN, the names of the Senator from Illinois (Mr. DURBIN) and the Senator from Massachusetts (Mr. KENNEDY) were added as cosponsors of S. 569, a bill to amend title XVIII of the Social Security Act to repeal the medicare outpatient rehabilitation therapy caps.

S. 589

At the request of Mr. AKAKA, the name of the Senator from Kansas (Mr. BROWNBACK) was added as a cosponsor of S. 589, a bill to strengthen and improve the management of national security, encourage Government service in areas of critical national security,

and to assist government agencies in addressing deficiencies in personnel possessing specialized skills important to national security and incorporating the goals and strategies for recruitment and retention for such skilled personnel into the strategic and performance management systems of Federal agencies.

S. 595

At the request of Mr. HATCH, the names of the Senator from Florida (Mr. NELSON) and the Senator from Virginia (Mr. WARNER) were added as cosponsors of S. 595, a bill to amend the Internal Revenue Code of 1986 to repeal the required use of certain principal repayments on mortgage subsidy bond financings to redeem bonds, to modify the purchase price limitation under mortgage subsidy bond rules based on median family income, and for other purposes.

S. 608

At the request of Mr. REED, the name of the Senator from New York (Mrs. CLINTON) was added as a cosponsor of S. 608, a bill to provide for personnel preparation, enhanced support and training for beginning special educators, and professional development of special educators, general educators, and early intervention personnel.

S. 609

At the request of Mr. LEAHY, the name of the Senator from Florida (Mr. GRAHAM) was added as a cosponsor of S. 609, a bill to amend the Homeland Security Act of 2002 (Public Law 107-296) to provide for the protection of voluntarily furnished confidential information, and for other purposes.

S. 647

At the request of Mr. KENNEDY, the name of the Senator from Nevada (Mr. REID) was added as a cosponsor of S. 647, a bill to amend title 10, United States Code, to provide for Department of Defense funding of continuation of health benefits plan coverage for certain Reserves called or ordered to active duty and their dependents, and for other purposes.

S. 678

At the request of Mr. AKAKA, the name of the Senator from Utah (Mr. HATCH) was added as a cosponsor of S. 678, a bill to amend chapter 10 of title 39, United States Code, to include postmasters and postmasters organizations in the process for the development and planning of certain policies, schedules, and programs, and for other purposes.

S. 704

At the request of Ms. COLLINS, the name of the Senator from Nebraska (Mr. NELSON) was added as a cosponsor of S. 704, a bill to amend title 10, United States Code, to increase the amount of the death gratuity payable with respect to deceased members of the Armed Forces.

S. 728

At the request of Mr. COLEMAN, the name of the Senator from Georgia (Mr. CHAMBLISS) was added as a cosponsor of

S. 728, a bill to reimburse the airline industry for homeland security costs, and for other purposes.

S. 731

At the request of Mr. BIDEN, the names of the Senator from Ohio (Mr. DEWINE) and the Senator from Wisconsin (Mr. FEINGOLD) were added as cosponsors of S. 731, a bill to prohibit fraud and related activity in connection with authentication features, and for other purposes.

S. 737

At the request of Mr. DURBIN, the name of the Senator from Louisiana (Ms. LANDRIEU) was added as a cosponsor of S. 737, a bill to amend title 37, United States Code, to increase the rate of imminent danger special pay and the amount of the family separation allowance.

S. RES. 52

At the request of Mr. CAMPBELL, the name of the Senator from Washington (Ms. CANTWELL) was added as a cosponsor of S. Res. 52, a resolution recognizing the social problem of child abuse and neglect, and supporting efforts to enhance public awareness of the problem.

S. RES. 82

At the request of Mr. BROWNBACK, the name of the Senator from Pennsylvania (Mr. SANTORUM) was added as a cosponsor of S. Res. 82, a resolution expressing the sense of the Senate concerning the continuous repression of freedoms within Iran and of individual human rights abuses, particularly with regard to women.

#### STATEMENTS ON INTRODUCED BILLS AND JOINT RESOLUTIONS

By Mr. DASCHLE (for Mr. EDWARDS):

S. 743. A bill to designate a building that houses the operations of the University Park United States Postal Service in Charlotte, North Carolina, as the "Jim Richardson Post Office Building"; to the Committee on Governmental Affairs.

Mr. DASCHLE. Mr. President, I rise today to introduce the "James F. Richardson Post Office Act of 2003." This measure would name the University Park Post Office in Charlotte, NC, after a man who has come to mean so much to the City of Charlotte, Mecklenburg County and the State of North Carolina. His record of public service goes back 60 years.

A Charlotte native, Jim Richardson graduated from Second War High School, the only high school in the area African Americans were allowed to attend. In a separate and unequal society he learned early on the importance of character and serving the public good. Our World War II veterans are said to be the greatest generation. As part of that generation Jim Richardson entered the United States Navy and served our country honorably in the South Pacific theater during World War II. It is with character and a deep

and abiding hope for a better future that a man such as Jim Richardson fought for his country only to return to a society that did not afford all that was allowed them under the Constitution of the United States.

After the war, Jim returned to Charlotte and entered Johnson C. Smith University. He graduated with a degree in Physical Education and minored in General Sciences. His Post Office career began in 1949 as a postal clerk in Charlotte. With the railroads still being the dominant form of transporting the mail, Jim transferred to the Railway Postal Service. When he returned to the Charlotte Post Office years later he had risen through the ranks to having held several supervisory positions. With 33 years of service in the Federal Government, he retired as the US Postmaster in Mt. Holly, NC.

Now, that would be a full career for most individuals. What I have not mentioned is that Jim Richardson was an elected official having served distinguishably in both the North Carolina State House and State Senate. It was here that this man whose family taught him the mantra "do good for others and goodness will return to you" continued his advocacy for those who needed it most. These were often the poor, minorities and the elderly. Jim's legislative record reflected his life's experiences. When he retired from the State Senate, he was a role model for elected officials of both parties. I include myself as being one who looks to Jim Richardson not on the issues of the day, but on the manner in which we conduct ourselves in the daily business of serving the people who elected us.

Again, you would think this would be enough public service for most people. Not for Jim. He returned from the State Legislature to Charlotte and was elected as a Mecklenburg County Commissioner. I came to know him during this his third career. When I called on him for advice and counsel, he opened the wealth of his life's experiences to me. He also opened his home where I stayed during my campaign for the Senate seat. I learned from the man and about him. He and his wife Mary are revered for so many of their contributions to the community. Chief among them is their work on HIV/AIDS awareness among young people. Their hope is to save lives and spare families the experience of losing a loved one to this dreaded disease.

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

S. 743

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

**SECTION 1. DESIGNATION OF JIM RICHARDSON POST OFFICE BUILDING.**

The building that houses operations of the University Park United States Postal Service, located at 2127 Beattys Ford Road, in Charlotte, North Carolina (or any other building to which the University Park United States Postal Service may relocate

after the date of enactment of this Act), shall be known and designated as the "Jim Richardson Post Office Building".

**SEC. 2. REFERENCES.**

Any reference in a law, map, regulation, document, paper, or other record of the United States to the annex to the building referred to in section 1 shall be deemed to be a reference to the Jim Richardson Post Office Building.

By Mrs. FEINSTEIN:

S. 745. A bill to require the consent of an individual prior to the sale and marketing of such individual's personally identifiable information, and for other purposes; to the Committee on the Judiciary.

Mrs. FEINSTEIN. Mr. President, I am pleased to introduce the "Privacy Act of 2003."

This legislation would establish, for the first time, a comprehensive national system of privacy protection.

It would: require companies to gain consumers' written consent prior to selling their most sensitive personal information including personal health information, financial information, Social Security numbers, and drivers' license data; and require companies to provide consumers' notice and an opportunity to refuse to allow their less sensitive personal information to be sold.

Simply put, this legislation would give consumers more control over how their personal information is used.

The personal information of today's consumer is too vulnerable to abuse. With access to sensitive data so widely available—often just at the touch of a keyboard—it is easy to understand why identity theft has become one of the country's fastest growing crimes.

Recent statistics on the growth of identity theft suggest we have no time to waste in protecting personal privacy.

Identity theft is the number one consumer complaint reported to the Federal Trade Commission. American consumers filed approximately 163,000 identity theft complaints with the FTC in 2002. Fully 43 percent of all the complaints the FTC receives are about identity theft.

An estimated 700,000 cases of identity theft occur each year. The average victim spends an average of 175 hours over a two-year period clearing off an average of \$17,000 fraud off their credit reports.

My own State, California, has more victims than any other state. The FTC recorded 30,738 identity theft cases last year from California consumers alone.

While modern technology has increased the threat to personal security and privacy, the protections for individual privacy have not kept pace. Our country's privacy laws form an incomplete and inconsistent patchwork.

For example, Americans enjoy the highest level of privacy protection concerning the names of the movies they rent at a video store. But, at the same time, it is perfectly legal to sell another person's Social Security number over the Internet.

The Privacy Act would establish a Federal privacy standard that adjusts the level of privacy protection according to the sensitivity of the information at issue.

The legislation provides the highest level of protection for a person's most sensitive data—personal financial data, health data, driver's license information, and Social Security numbers.

For this sensitive data, the bill gives the individual ultimate control over whether or not his or her information is shared. If an individual does not actively decide to permit sharing of personal data, the data is not disclosed.

Specifically, this legislation tightens the privacy provisions of the Financial Services Modernization Act, commonly known as the Gramm-Leach-Bliley Act. Under Gramm-Leach-Bliley, a bank can share a customer's personal information with other companies so long as it gives consumers notice and the right to opt-out of the data sharing.

The problem with opt-out is that most people toss out their privacy notices from banks along with the rest of the unrelenting pile of commercial solicitations they receive. Since the passage of Gramm-Leach-Bliley, banks have sent out over one billion privacy notices.

According to available published information, fewer than 5 percent of bank customers have opted out of sharing their personal information, and for many financial institutions, the response rate has been less than one percent.

It is not surprising that consumers do not respond overwhelmingly to these notices, since, by some estimates, the average American household received a dozen of these notices. A consumer should not have the burden of constantly monitoring how his or her most sensitive personal information is shared with other companies.

Accordingly, the Privacy Act prohibits the sale or disclosure of sensitive personal financial information to third parties unless the consumer affirmatively consents or opts in.

This legislation also toughens Federal financial privacy laws for affiliate sharing and joint marketing. An affiliate is a company that is linked by common ownership with another company. Under Federal law, a bank can share with affiliates or joint marketing partners regardless of whether the consumer wants this information shared.

The Privacy Act of 2003 would require that banks give consumers the option of opting out of the sharing of their personal financial information with the bank's affiliates or joint partners.

Some banks argue that affiliates are just branches of an organization, and a bank should for efficiency purposes be able to share data within the entire organization. In an era where a bank had one or two affiliates, that might be true.

But, now, some companies are so big that if a customer has no control over

affiliate sharing, then the customer is unable to prevent the disclosure of their data to hundreds of companies. For example, in recent testimony before Congress, U.S. PIRG reported that Citibank has 2,761 affiliates, Key Bank had 871 affiliates, and Bank of America has 1,576 affiliates.

Similarly, a customer must be able to restrict a bank's sharing of personal information with its joint venture partners if the customer wants to maintain control over his personal information.

I would also like to describe several other key components of the financial privacy section.

The bill prohibits banks from denying a customer a financial product or financial service just because the customer chooses to not disclose his personal information to third parties, affiliates, or joint venture partners. However, the bill does allow banks to offer incentives to customers to encourage them to permit the sharing of their personal information.

Additionally, the bill permits banks to disclose, but not sell, personal information to third parties for vital public interest purposes such as identifying or locating missing and abducted children, witnesses, criminals and fugitives, parents delinquent in child support payments, organ and bone marrow donors, pension fund beneficiaries, and missing heirs.

Just as with financial data, personal health data deserves the most stringent privacy protections.

The recently adopted Department of Health and Human Services privacy regulations set a basic opt-in framework for disclosure of health information. But more can be done to protect patient privacy.

The regulations only prohibit "covered entities"—namely health insurers, health providers, and health care clearinghouses—from selling a patient's health information without that patient's prior consent.

Meanwhile, non-covered entities such as business associates, health researchers, schools or universities, and life insurers are not subject to this opt-in requirement, except through contractual arrangements.

This legislation would preserve the privacy of health information wherever the information is sold. Any business associate, life insurer, school or non-covered entity trying to sell or market protected health information would, like covered entities, have to get the patient's prior consent.

Drivers' license data also is given the strongest level of protection under this bill.

With its recent amendments, the Driver's Privacy Protection Act, DPPA, offers some meaningful protections for drivers privacy.

For example, under the DPPA, a State Department of Motor Vehicles must obtain the prior consent, Opt-in, of the driver before "highly sensitive information"—defined as the driver's

photograph, image, Social Security number, medical or disability information—can be disclosed to a third party.

However, loopholes remain. Other sensitive information found on a driver's license deserves equal protection.

The Privacy Act would expand the definition of "highly sensitive information" to include a physical copy of a driver's license, the driver identification number, birth date, information on the driver's physical characteristics and any biometric identifiers, such as a fingerprint, that are found on the driver's license.

Thus, this bill would ensure consumers have control over how their motor vehicle records and driver's license data are used.

I would like to take a moment to highlight the Social Security number section of the privacy bill, which reflects over four years of negotiation with Senator HATCH, Senator GREGG, Senator GRASSLEY, Senator BAUCUS, and other Senate colleagues. I have also introduced this section as a stand-alone bill, Senate bill 228.

It is crucial to protect Social Security numbers because the numbers are the key to a person's identity. Many identity theft cases start with the theft of a Social Security number. Once a thief has access to a victim's Social Security number, it is only a short step to acquiring credit cards, driver's licenses, or other crucial identification documents.

Not surprisingly, members of the public have flooded our Federal agencies with pleas for assistance. Reports to the Social Security Administration of Social Security number misuse have increased from 7,868 in 1997 to 73,000 in 2002—an astonishing increase of over 800%.

The Feinstein/Gregg compromise bars the sale or display of Social Security numbers to the public except in a very narrow set of circumstances.

Display or sale is permitted if the Social Security number holder consents or if there are compelling public safety needs.

Government entities will have to redact Social Security numbers from electronic records that are readily available to the public on the Internet.

Moreover, State governments will no longer be permitted to use the Social Security number as the default driver's license number.

The legislation, however, recognizes that some industries rely on Social Security numbers to exchange information between databases and complete identification verification necessary for certain transactions.

Thus, the bill directs the Attorney General to develop regulations allowing for the sale or purchase of Social Security Numbers to facilitate business-to-business and business-to-government transactions so long as businesses put appropriate safeguards in place and do not permit public access to the number.

Recognizing that not all personal information merits the same restric-

tions, the bill permits businesses to collect and sell nonsensitive personal information, *e.g.*, name, phone number, address, to third parties so long as they give customers notice and the opportunity to opt-out of the sale.

The opt-out standard for non-sensitive information means that if a person fills out a warranty card, signs up for a computer service, or submits an entry for a sweepstakes, the business must notify him before it sells his personal information to other businesses or marketers.

This framework guarantees basic privacy protections for consumers without unduly impacting commerce.

To further minimize the regulatory burden of these privacy rules, the bill sets up a safe harbor so that industries and industry-sponsored seal programs which have already adopted Notice-and-Opt Out information policies, will be exempt from the regulatory requirements of the legislation.

To ensure uniformity of the laws across all 50 states, the bill preempts inconsistent state laws regarding the treatment of non-sensitive information.

A jumbled patchwork of State privacy laws helps neither businesses nor consumers. Consumers will have confused expectations about what information is protected.

Another distinguishing characteristic of the Privacy Act of 2003 is that it protects the privacy of information regardless of the medium through which it is collected.

Other privacy proposals have tried to confine privacy legislation to the Internet.

These proposals unfairly discriminate against high technology users. Put simply, companies and other entities can misuse personal information from off-line sources just as easily as with on-line sources.

For example, telemarketers who besiege consumers with phone calls during the dinner hour do not typically get customer information from the Internet. Much of the identifying information used to make these calls comes from consumers filling out and mailing back warranty and registration cards.

Regardless of how information is collected, it should get equal protection.

This legislation codifies steps Congress can take to protect citizens from identity thieves and other predators of personal information.

It restores to an individual more control over his or her most sensitive personal information such as Social Security numbers, health information, and financial information. It also sets reasonable guidelines for businesses that handle our personal information every day.

A byproduct of our information economy—personal information is much more vulnerable to exploitation than ever before.

Every American has a fundamental right to privacy, no matter how fast our technology grows or changes. A

person should be able to have control over how their most sensitive personal information is used.

But our right to privacy only will remain vital, if we take strong action to protect it.

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

I look forward to working with my colleagues to enact the Privacy Act of 2003.

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

S. 745

*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 “Privacy Act of 2003”.

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

Sec. 1. Short title; table of contents.

#### TITLE I—COMMERCIAL SALE AND MARKETING OF PERSONALLY IDENTIFIABLE INFORMATION

Sec. 101. Collection and distribution of personally identifiable information.

Sec. 102. Enforcement.

Sec. 103. Safe harbor.

Sec. 104. Definitions.

Sec. 105. Preemption.

Sec. 106. Effective Date.

#### TITLE II—SOCIAL SECURITY NUMBER MISUSE PREVENTION

Sec. 201. Findings.

Sec. 202. Prohibition of the display, sale, or purchase of social security numbers.

Sec. 203. Application of prohibition of the display, sale, or purchase of social security numbers to public records.

Sec. 204. Rulemaking authority of the Attorney General.

Sec. 205. Treatment of social security numbers on government documents.

Sec. 206. Limits on personal disclosure of a social security number for consumer transactions.

Sec. 207. Extension of civil monetary penalties for misuse of a social security number.

Sec. 208. Criminal penalties for the misuse of a social security number.

Sec. 209. Civil actions and civil penalties.

Sec. 210. Federal injunctive authority.

#### TITLE III—LIMITATIONS ON SALE AND SHARING OF NONPUBLIC PERSONAL FINANCIAL INFORMATION

Sec. 301. Definition of sale.

Sec. 302. Rules applicable to sale of nonpublic personal information.

Sec. 303. Exceptions to disclosure prohibition.

Sec. 304. Conforming amendments.

Sec. 305. Regulatory authority.

Sec. 306. Effective date.

#### TITLE IV—LIMITATIONS ON THE PROVISION OF PROTECTED HEALTH INFORMATION

Sec. 401. Definitions.

Sec. 402. Prohibition against selling protected health information.

Sec. 403. Authorization for sale or marketing of protected health information by noncovered entities.

Sec. 404. Prohibition against retaliation.

Sec. 405. Rule of construction.

Sec. 406. Regulations.

Sec. 407. Enforcement.

#### TITLE V—DRIVER'S LICENSE PRIVACY

Sec. 501. Driver's license privacy.

#### TITLE VI—MISCELLANEOUS

Sec. 601. Enforcement by State Attorneys General.

Sec. 602. Federal injunctive authority.

#### TITLE I—COMMERCIAL SALE AND MARKETING OF PERSONALLY IDENTIFIABLE INFORMATION

##### SEC. 101. COLLECTION AND DISTRIBUTION OF PERSONALLY IDENTIFIABLE INFORMATION.

(a) PROHIBITION.—

(1) IN GENERAL.—It is unlawful for a commercial entity to collect personally identifiable information and disclose such information to any nonaffiliated third party for marketing purposes or sell such information to any nonaffiliated third party, unless the commercial entity provides—

(A) notice to the individual to whom the information relates in accordance with the requirements of subsection (b); and

(B) an opportunity for such individual to restrict the disclosure or sale of such information.

(2) EXCEPTION.—A commercial entity may collect personally identifiable information and use such information to market to potential customers such entity's product.

(b) NOTICE.—

(1) IN GENERAL.—A notice under subsection (a) shall contain statements describing the following:

(A) The identity of the commercial entity collecting the personally identifiable information.

(B) The types of personally identifiable information that are being collected on the individual.

(C) How the commercial entity may use such information.

(D) A description of the categories of potential recipients of such personally identifiable information.

(E) Whether the individual is required to provide personally identifiable information in order to do business with the commercial entity.

(F) How an individual may decline to have such personally identifiable information used or sold as described in subsection (a).

(2) TIME OF NOTICE.—Notice shall be conveyed prior to the sale or use of the personally identifiable information as described in subsection (a) in such a manner as to allow the individual a reasonable period of time to consider the notice and limit such sale or use.

(3) MEDIUM OF NOTICE.—The medium for providing notice must be—

(A) the same medium in which the personally identifiable information is or will be collected, or a medium approved by the individual; or

(B) in the case of oral communication, notice may be conveyed orally or in writing.

(4) FORM OF NOTICE.—The notice shall be clear and conspicuous.

(c) OPT-OUT.—

(1) OPPORTUNITY TO OPT-OUT OF SALE OR MARKETING.—The opportunity provided to limit the sale of personally identifiable information to nonaffiliated third parties or the disclosure of such information for marketing purposes, shall be easy to use, accessible and available in the medium the information is collected, or in a medium approved by the individual.

(2) DURATION OF LIMITATION.—An individual's limitation on the sale or marketing of personally identifiable information shall be considered permanent, unless otherwise specified by the individual.

(3) REVOCATION OF CONSENT.—After an individual grants consent to the use of that individual's personally identifiable information, the individual may revoke the consent at any time, except to the extent that the commercial entity has taken action in reliance thereon. The commercial entity shall provide the individual an opportunity to revoke consent that is easy to use, accessible, and available in the medium the information was or is collected.

(4) NOT APPLICABLE.—This section shall not apply to disclosure of personally identifiable information—

(A) that is necessary to facilitate a transaction specifically requested by the consumer;

(B) is used for the sole purpose of facilitating this transaction; and

(C) in which the entity receiving or obtaining such information is limited, by contract, to use such information for the purpose of completing the transaction.

##### SEC. 102. ENFORCEMENT.

(a) IN GENERAL.—In accordance with the provisions of this section, the Federal Trade Commission shall have the authority to enforce any violation of section 101 of this Act.

(b) VIOLATIONS.—The Federal Trade Commission shall treat a violation of section 101 as a violation of a rule under section 18a(a)(1)(B) of the Federal Trade Commission Act (15 U.S.C. 57a(a)(1)(B)).

(c) TRANSFER OF ENFORCEMENT AUTHORITY.—The Federal Trade Commission shall promulgate rules in accordance with section 553 of title 5, United States Code, allowing for the transfer of enforcement authority from the Federal Trade Commission to a Federal agency regarding section 101 of this Act. The Federal Trade Commission may permit a Federal agency to enforce any violation of section 101 if such agency submits a written request to the Commission to enforce such violations and includes in such request—

(1) a description of the entities regulated by such agency that will be subject to the provisions of section 101;

(2) an assurance that such agency has sufficient authority over the entities to enforce violations of section 101; and

(3) a list of proposed rules that such agency shall use in regulating such entities and enforcing section 101.

(d) ACTIONS BY THE COMMISSION.—Absent transfer of enforcement authority to a Federal agency under subsection (c), the Federal Trade Commission shall prevent any person from violating section 101 in the same manner, by the same means, and with the same jurisdiction, powers, and duties as provided to such Commission under the Federal Trade Commission Act (15 U.S.C. 41 et seq.). Any entity that violates section 101 is subject to the penalties and entitled to the privileges and immunities provided in such Act in the same manner, by the same means, and with the same jurisdiction, power, and duties under such Act.

(e) RELATIONSHIP TO OTHER LAWS.—

(1) COMMISSION AUTHORITY.—Nothing contained in this title shall be construed to limit authority provided to the Commission under any other law.

(2) COMMUNICATIONS ACT.—Nothing in section 101 requires an operator of a website to take any action that is inconsistent with the requirements of section 222 or 631 of the Communications Act of 1934 (47 U.S.C. 222 and 551).

(3) OTHER ACTS.—Nothing in this title is intended to affect the applicability or the enforceability of any provision of, or any amendment made by—

(A) the Children's Online Privacy Protection Act of 1998 (15 U.S.C. 6501 et seq.);

(B) title V of the Gramm-Leach-Bliley Act; (C) the Health Insurance Portability and Accountability Act of 1996; or

(D) the Fair Credit Reporting Act.

(f) PUBLIC RECORDS.—Nothing in this title shall be construed to restrict commercial entities from obtaining or disclosing personally identifying information from public records.

(g) CIVIL PENALTIES.—In addition to any other penalty applicable to a violation of section 101(a), a penalty of up to \$25,000 may be issued for each violation.

(h) ENFORCEMENT REGARDING PROGRAMS.—

(1) IN GENERAL.—A Federal agency or department providing financial assistance to any entity required to comply with section 101 of this Act shall issue regulations requiring that such entity comply with such section or forfeit some or all of such assistance. Such regulations shall prescribe sanctions for noncompliance, require that such department or agency provide notice of failure to comply with such section prior to any action being taken against such recipient, and require that a determination be made prior to any action being taken against such recipient that compliance cannot be secured by voluntary means.

(2) FEDERAL FINANCIAL ASSISTANCE.—The term “Federal financial assistance” means assistance through a grant, cooperative agreement, loan, or contract other than a contract of insurance or guaranty.

#### SEC. 103. SAFE HARBOR.

A commercial entity may not be held to have violated any provision of this title if such entity complies with self-regulatory guidelines that—

“(1) are issued by seal programs or representatives of the marketing or online industries or by any other person; and

“(2) are approved by the Federal Trade Commission, after public comment has been received on such guidelines by the Commission, as meeting the requirements of this title.

#### SEC. 104. DEFINITIONS.

In this title:

(1) COMMERCIAL ENTITY.—The term “commercial entity”—

(A) means any person offering products or services involving commerce—

(i) among the several States or with 1 or more foreign nations;

(ii) in any territory of the United States or in the District of Columbia, or between any such territory and—

(I) another such territory; or

(II) any State or foreign nation; or

(iii) between the District of Columbia and any State, territory, or foreign nation; and (B) does not include—

(i) any nonprofit entity that would otherwise be exempt from coverage under section 5 of the Federal Trade Commission Act (15 U.S.C. 45);

(ii) any financial institution that is subject to title V of the Gramm-Leach-Bliley Act (15 U.S.C. 6801 et seq.); or

(iii) any group health plan, health insurance issuer, or other entity that is subject to the Health Insurance Portability and Accountability Act of 1996 (42 U.S.C. 201 note).

(2) COMMISSION.—The term “Commission” means the Federal Trade Commission.

(3) INDIVIDUAL.—The term “individual” means a person whose personally identifying information has been, is, or will be collected by a commercial entity.

(4) MARKETING.—The term “marketing” means to make a communication about a product or service a purpose of which is to encourage recipients of the communication to purchase or use the product or service.

(5) MEDIUM.—The term “medium” means any channel or system of communication in-

cluding oral, written, and online communication.

(6) NONAFFILIATED THIRD PARTY.—The term “nonaffiliated third party” means any entity that is not related by common ownership or affiliated by corporate control with, the commercial entity, but does not include a joint employee of such institution.

(7) PERSONALLY IDENTIFIABLE INFORMATION.—The term “personally identifiable information” means individually identifiable information about the individual that is collected including—

(A) a first, middle, or last name, whether given at birth or adoption, assumed, or legally changed;

(B) a home or other physical address, including the street name, zip code, and name of a city or town;

(C) an e-mail address;

(D) a telephone number;

(E) a photograph or other form of visual identification;

(F) a birth date, birth certificate number, or place of birth for that person; or

(G) information concerning the individual that is combined with any other identifier in this paragraph.

(8) SALE; SELL; SOLD.—The terms “sale”, “sell”, and “sold”, with respect to personally identifiable information, mean the exchanging of such information for any thing of value, directly or indirectly, including the licensing, bartering, or renting of such information.

(9) WRITING.—The term “writing” means writing in either a paper-based or computer-based form, including electronic and digital signatures.

#### SEC. 105. PREEMPTION.

The provisions of this title shall supersede any statutory and common law of States and their political subdivisions insofar as that law may now or hereafter relate to the—

(1) collection and disclosure of personally identifiable information for marketing purposes; and

(2) collection and sale of personally identifiable information.

#### SEC. 106. EFFECTIVE DATE.

This title and the amendments made by this title shall take effect 1 year after the date of enactment of this Act.

### TITLE II—SOCIAL SECURITY NUMBER MISUSE PREVENTION

#### SEC. 201. FINDINGS.

Congress makes the following findings:

(1) The inappropriate display, sale, or purchase of social security numbers has contributed to a growing range of illegal activities, including fraud, identity theft, and, in some cases, stalking and other violent crimes.

(2) While financial institutions, health care providers, and other entities have often used social security numbers to confirm the identity of an individual, the general display to the public, sale, or purchase of these numbers has been used to commit crimes, and also can result in serious invasions of individual privacy.

(3) The Federal Government requires virtually every individual in the United States to obtain and maintain a social security number in order to pay taxes, to qualify for social security benefits, or to seek employment. An unintended consequence of these requirements is that social security numbers have become one of the tools that can be used to facilitate crime, fraud, and invasions of the privacy of the individuals to whom the numbers are assigned. Because the Federal Government created and maintains this system, and because the Federal Government does not permit individuals to exempt themselves from those requirements, it is appropriate for the Federal Government to take

steps to stem the abuse of social security numbers.

(4) The display, sale, or purchase of social security numbers in no way facilitates uninhibited, robust, and wide-open public debate, and restrictions on such display, sale, or purchase would not affect public debate.

(5) No one should seek to profit from the display, sale, or purchase of social security numbers in circumstances that create a substantial risk of physical, emotional, or financial harm to the individuals to whom those numbers are assigned.

(6) Consequently, this title provides each individual that has been assigned a social security number some degree of protection from the display, sale, and purchase of that number in any circumstance that might facilitate unlawful conduct.

#### SEC. 202. PROHIBITION OF THE DISPLAY, SALE, OR PURCHASE OF SOCIAL SECURITY NUMBERS.

(a) PROHIBITION.—

(1) IN GENERAL.—Chapter 47 of title 18, United States Code, is amended by inserting after section 1028 the following:

##### “§ 1028A. Prohibition of the display, sale, or purchase of social security numbers

“(a) DEFINITIONS.—In this section:

“(1) DISPLAY.—The term ‘display’ means to intentionally communicate or otherwise make available (on the Internet or in any other manner) to the general public an individual’s social security number.

“(2) PERSON.—The term ‘person’ means any individual, partnership, corporation, trust, estate, cooperative, association, or any other entity.

“(3) PURCHASE.—The term ‘purchase’ means providing directly or indirectly, anything of value in exchange for a social security number.

“(4) SALE.—The term ‘sale’ means obtaining, directly or indirectly, anything of value in exchange for a social security number.

“(5) STATE.—The term ‘State’ means any State of the United States, the District of Columbia, Puerto Rico, the Northern Mariana Islands, the United States Virgin Islands, Guam, American Samoa, and any territory or possession of the United States.

“(b) LIMITATION ON DISPLAY.—Except as provided in section 1028B, no person may display any individual’s social security number to the general public without the affirmatively expressed consent of the individual.

“(c) LIMITATION ON SALE OR PURCHASE.—Except as otherwise provided in this section, no person may sell or purchase any individual’s social security number without the affirmatively expressed consent of the individual.

“(d) PREREQUISITES FOR CONSENT.—In order for consent to exist under subsection (b) or (c), the person displaying or seeking to display, selling or attempting to sell, or purchasing or attempting to purchase, an individual’s social security number shall—

“(1) inform the individual of the general purpose for which the number will be used, the types of persons to whom the number may be available, and the scope of transactions permitted by the consent; and

“(2) obtain the affirmatively expressed consent (electronically or in writing) of the individual.

“(e) EXCEPTIONS.—Nothing in this section shall be construed to prohibit or limit the display, sale, or purchase of a social security number—

“(1) required, authorized, or excepted under any Federal law;

“(2) for a public health purpose, including the protection of the health or safety of an individual in an emergency situation;

“(3) for a national security purpose;

“(4) for a law enforcement purpose, including the investigation of fraud and the enforcement of a child support obligation;

“(5) if the display, sale, or purchase of the number is for a use occurring as a result of an interaction between businesses, governments, or business and government (regardless of which entity initiates the interaction), including, but not limited to—

“(A) the prevention of fraud (including fraud in protecting an employee’s right to employment benefits);

“(B) the facilitation of credit checks or the facilitation of background checks of employees, prospective employees, or volunteers;

“(C) the retrieval of other information from other businesses, commercial enterprises, government entities, or private non-profit organizations; or

“(D) when the transmission of the number is incidental to, and in the course of, the sale, lease, franchising, or merger of all, or a portion of, a business;

“(6) if the transfer of such a number is part of a data matching program involving a Federal, State, or local agency; or

“(7) if such number is required to be submitted as part of the process for applying for any type of Federal, State, or local government benefit or program;

except that, nothing in this subsection shall be construed as permitting a professional or commercial user to display or sell a social security number to the general public.

“(f) LIMITATION.—Nothing in this section shall prohibit or limit the display, sale, or purchase of social security numbers as permitted under title V of the Gramm-Leach-Bliley Act, or for the purpose of affiliate sharing as permitted under the Fair Credit Reporting Act, except that no entity regulated under such Acts may make social security numbers available to the general public, as may be determined by the appropriate regulators under such Acts. For purposes of this subsection, the general public shall not include affiliates or unaffiliated third-party business entities as may be defined by the appropriate regulators.”.

(2) CONFORMING AMENDMENT.—The chapter analysis for chapter 47 of title 18, United States Code, is amended by inserting after the item relating to section 1028 the following:

“1028A. Prohibition of the display, sale, or purchase of social security numbers.”.

(b) STUDY; REPORT.—

(1) IN GENERAL.—The Attorney General shall conduct a study and prepare a report on all of the uses of social security numbers permitted, required, authorized, or excepted under any Federal law. The report shall include a detailed description of the uses allowed as of the date of enactment of this Act and shall evaluate whether such uses should be continued or discontinued by appropriate legislative action.

(2) REPORT.—Not later than 1 year after the date of enactment of this Act, the Attorney General shall report to Congress findings under this subsection. The report shall include such recommendations for legislation based on criteria the Attorney General determines to be appropriate.

(c) EFFECTIVE DATE.—The amendments made by this section shall take effect on the date that is 30 days after the date on which the final regulations promulgated under section 5 are published in the Federal Register.

**SEC. 203. APPLICATION OF PROHIBITION OF THE DISPLAY, SALE, OR PURCHASE OF SOCIAL SECURITY NUMBERS TO PUBLIC RECORDS.**

(a) PUBLIC RECORDS EXCEPTION.—

(1) IN GENERAL.—Chapter 47 of title 18, United States Code (as amended by section

3(a)(1)), is amended by inserting after section 1028A the following:

**“§ 1028B. Display, sale, or purchase of public records containing social security numbers**

“(a) DEFINITION.—In this section, the term ‘public record’ means any governmental record that is made available to the general public.

“(b) IN GENERAL.—Except as provided in subsections (c), (d), and (e), section 1028A shall not apply to a public record.

“(c) PUBLIC RECORDS ON THE INTERNET OR IN AN ELECTRONIC MEDIUM.—

“(1) IN GENERAL.—Section 1028A shall apply to any public record first posted onto the Internet or provided in an electronic medium by, or on behalf of a government entity after the date of enactment of this section, except as limited by the Attorney General in accordance with paragraph (2).

“(2) EXCEPTION FOR GOVERNMENT ENTITIES ALREADY PLACING PUBLIC RECORDS ON THE INTERNET OR IN ELECTRONIC FORM.—Not later than 60 days after the date of enactment of this section, the Attorney General shall issue regulations regarding the applicability of section 1028A to any record of a category of public records first posted onto the Internet or provided in an electronic medium by, or on behalf of a government entity prior to the date of enactment of this section. The regulations will determine which individual records within categories of records of these government entities, if any, may continue to be posted on the Internet or in electronic form after the effective date of this section. In promulgating these regulations, the Attorney General may include in the regulations a set of procedures for implementing the regulations and shall consider the following:

“(A) The cost and availability of technology available to a governmental entity to redact social security numbers from public records first provided in electronic form after the effective date of this section.

“(B) The cost or burden to the general public, businesses, commercial enterprises, non-profit organizations, and to Federal, State, and local governments of complying with section 1028A with respect to such records.

“(C) The benefit to the general public, businesses, commercial enterprises, non-profit organizations, and to Federal, State, and local governments if the Attorney General were to determine that section 1028A should apply to such records.

Nothing in the regulation shall permit a public entity to post a category of public records on the Internet or in electronic form after the effective date of this section if such category had not been placed on the Internet or in electronic form prior to such effective date.

“(d) HARVESTED SOCIAL SECURITY NUMBERS.—Section 1028A shall apply to any public record of a government entity which contains social security numbers extracted from other public records for the purpose of displaying or selling such numbers to the general public.

“(e) ATTORNEY GENERAL RULEMAKING ON PAPER RECORDS.—

“(1) IN GENERAL.—Not later than 60 days after the date of enactment of this section, the Attorney General shall determine the feasibility and advisability of applying section 1028A to the records listed in paragraph (2) when they appear on paper or on another nonelectronic medium. If the Attorney General deems it appropriate, the Attorney General may issue regulations applying section 1028A to such records.

“(2) LIST OF PAPER AND OTHER NONELECTRONIC RECORDS.—The records listed in this paragraph are as follows:

“(A) Professional or occupational licenses.

“(B) Marriage licenses.

“(C) Birth certificates.

“(D) Death certificates.

“(E) Other short public documents that display a social security number in a routine and consistent manner on the face of the document.

“(3) CRITERIA FOR ATTORNEY GENERAL REVIEW.—In determining whether section 1028A should apply to the records listed in paragraph (2), the Attorney General shall consider the following:

“(A) The cost or burden to the general public, businesses, commercial enterprises, non-profit organizations, and to Federal, State, and local governments of complying with section 1028A.

“(B) The benefit to the general public, businesses, commercial enterprises, non-profit organizations, and to Federal, State, and local governments if the Attorney General were to determine that section 1028A should apply to such records.”.

(2) CONFORMING AMENDMENT.—The chapter analysis for chapter 47 of title 18, United States Code (as amended by section 202(a)(2)), is amended by inserting after the item relating to section 1028A the following:

“1028B. Display, sale, or purchase of public records containing social security numbers.”.

(b) STUDY AND REPORT ON SOCIAL SECURITY NUMBERS IN PUBLIC RECORDS.—

(1) STUDY.—The Comptroller General of the United States shall conduct a study and prepare a report on social security numbers in public records. In developing the report, the Comptroller General shall consult with the Administrative Office of the United States Courts, State and local governments that store, maintain, or disseminate public records, and other stakeholders, including members of the private sector who routinely use public records that contain social security numbers.

(2) REPORT.—Not later than 1 year after the date of enactment of this Act, the Comptroller General of the United States shall submit to Congress a report on the study conducted under paragraph (1). The report shall include a detailed description of the activities and results of the study and recommendations for such legislative action as the Comptroller General considers appropriate. The report, at a minimum, shall include—

(A) a review of the uses of social security numbers in non-federal public records;

(B) a review of the manner in which public records are stored (with separate reviews for both paper records and electronic records);

(C) a review of the advantages or utility of public records that contain social security numbers, including the utility for law enforcement, and for the promotion of homeland security;

(D) a review of the disadvantages or drawbacks of public records that contain social security numbers, including criminal activity, compromised personal privacy, or threats to homeland security;

(E) the costs and benefits for State and local governments of removing social security numbers from public records, including a review of current technologies and procedures for removing social security numbers from public records; and

(F) an assessment of the benefits and costs to businesses, their customers, and the general public of prohibiting the display of social security numbers on public records (with separate assessments for both paper records and electronic records).

(c) EFFECTIVE DATE.—The prohibition with respect to electronic versions of new classes of public records under section 1028B(b) of title 18, United States Code (as added by subsection (a)(1)) shall not take effect until the

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

**SEC. 204. RULEMAKING AUTHORITY OF THE ATTORNEY GENERAL.**

(a) IN GENERAL.—Except as provided in subsection (b), the Attorney General may prescribe such rules and regulations as the Attorney General deems necessary to carry out the provisions of section 1028A(e)(5) of title 18, United States Code (as added by section 202(a)(1)).

(b) DISPLAY, SALE, OR PURCHASE RULEMAKING WITH RESPECT TO INTERACTIONS BETWEEN BUSINESSES, GOVERNMENTS, OR BUSINESS AND GOVERNMENT.—

(1) IN GENERAL.—Not later than 1 year after the date of enactment of this Act, the Attorney General, in consultation with the Commissioner of Social Security, the Chairman of the Federal Trade Commission, and such other heads of Federal agencies as the Attorney General determines appropriate, shall conduct such rulemaking procedures in accordance with subchapter II of chapter 5 of title 5, United States Code, as are necessary to promulgate regulations to implement and clarify the uses occurring as a result of an interaction between businesses, governments, or business and government (regardless of which entity initiates the interaction) permitted under section 1028A(e)(5) of title 18, United States Code (as added by section 202(a)(1)).

(2) FACTORS TO BE CONSIDERED.—In promulgating the regulations required under paragraph (1), the Attorney General shall, at a minimum, consider the following:

(A) The benefit to a particular business, to customers of the business, and to the general public of the display, sale, or purchase of an individual's social security number.

(B) The costs that businesses, customers of businesses, and the general public may incur as a result of prohibitions on the display, sale, or purchase of social security numbers.

(C) The risk that a particular business practice will promote the use of a social security number to commit fraud, deception, or crime.

(D) The presence of adequate safeguards and procedures to prevent—

(i) misuse of social security numbers by employees within a business; and

(ii) misappropriation of social security numbers by the general public, while permitting internal business uses of such numbers.

(E) The presence of procedures to prevent identity thieves, stalkers, and other individuals with ill intent from posing as legitimate businesses to obtain social security numbers.

**SEC. 205. TREATMENT OF SOCIAL SECURITY NUMBERS ON GOVERNMENT DOCUMENTS.**

(a) PROHIBITION OF USE OF SOCIAL SECURITY ACCOUNT NUMBERS ON CHECKS ISSUED FOR PAYMENT BY GOVERNMENTAL AGENCIES.—

(1) IN GENERAL.—Section 205(c)(2)(C) of the Social Security Act (42 U.S.C. 405(c)(2)(C)) is amended by adding at the end the following:

“(x) No Federal, State, or local agency may display the social security account number of any individual, or any derivative of such number, on any check issued for any payment by the Federal, State, or local agency.”.

(2) EFFECTIVE DATE.—The amendment made by this subsection shall apply with respect to violations of section 205(c)(2)(C)(x) of the Social Security Act (42 U.S.C. 405(c)(2)(C)(x)), as added by paragraph (1), occurring after the date that is 3 years after the date of enactment of this Act.

(b) PROHIBITION OF APPEARANCE OF SOCIAL SECURITY ACCOUNT NUMBERS ON DRIVER'S LICENSES OR MOTOR VEHICLE REGISTRATION.—

(1) IN GENERAL.—Section 205(c)(2)(C)(vi) of the Social Security Act (42 U.S.C. 405(c)(2)(C)(vi)) is amended—

(A) by inserting “(I)” after “(vi)”;

(B) by adding at the end the following:

“(II)(aa) An agency of a State (or political subdivision thereof), in the administration of any driver's license or motor vehicle registration law within its jurisdiction, may not display the social security account numbers issued by the Commissioner of Social Security, or any derivative of such numbers, on the face of any driver's license or motor vehicle registration or any other document issued by such State (or political subdivision thereof) to an individual for purposes of identification of such individual.

“(bb) Nothing in this subclause shall be construed as precluding an agency of a State (or political subdivision thereof), in the administration of any driver's license or motor vehicle registration law within its jurisdiction, from using a social security account number for an internal use or to link with the database of an agency of another State that is responsible for the administration of any driver's license or motor vehicle registration law.”.

(2) EFFECTIVE DATE.—The amendments made by this subsection shall apply with respect to licenses, registrations, and other documents issued or reissued after the date that is 1 year after the date of enactment of this Act.

(c) PROHIBITION OF INMATE ACCESS TO SOCIAL SECURITY ACCOUNT NUMBERS.—

(1) IN GENERAL.—Section 205(c)(2)(C) of the Social Security Act (42 U.S.C. 405(c)(2)(C)) (as amended by subsection (b)) is amended by adding at the end the following:

“(xi) No Federal, State, or local agency may employ, or enter into a contract for the use or employment of, prisoners in any capacity that would allow such prisoners access to the social security account numbers of other individuals. For purposes of this clause, the term ‘prisoner’ means an individual confined in a jail, prison, or other penal institution or correctional facility pursuant to such individual's conviction of a criminal offense.”.

(2) EFFECTIVE DATE.—The amendment made by this subsection shall apply with respect to employment of prisoners, or entry into contract with prisoners, after the date that is 1 year after the date of enactment of this Act.

**SEC. 206. LIMITS ON PERSONAL DISCLOSURE OF A SOCIAL SECURITY NUMBER FOR CONSUMER TRANSACTIONS.**

(a) IN GENERAL.—Part A of title XI of the Social Security Act (42 U.S.C. 1301 et seq.) is amended by adding at the end the following:

**“SEC. 1150A. LIMITS ON PERSONAL DISCLOSURE OF A SOCIAL SECURITY NUMBER FOR CONSUMER TRANSACTIONS.**

“(a) IN GENERAL.—A commercial entity may not require an individual to provide the individual's social security number when purchasing a commercial good or service or deny an individual the good or service for refusing to provide that number except—

“(1) for any purpose relating to—

“(A) obtaining a consumer report for any purpose permitted under the Fair Credit Reporting Act;

“(B) a background check of the individual conducted by a landlord, lessor, employer, voluntary service agency, or other entity as determined by the Attorney General;

“(C) law enforcement; or

“(D) a Federal, State, or local law requirement; or

“(2) if the social security number is necessary to verify the identity of the consumer to effect, administer, or enforce the specific transaction requested or authorized by the consumer, or to prevent fraud.

“(b) APPLICATION OF CIVIL MONEY PENALTIES.—A violation of this section shall be deemed to be a violation of section 1129(a)(3)(F).

“(c) APPLICATION OF CRIMINAL PENALTIES.—A violation of this section shall be deemed to be a violation of section 208(a)(8).

“(d) LIMITATION ON CLASS ACTIONS.—No class action alleging a violation of this section shall be maintained under this section by an individual or any private party in Federal or State court.

“(e) STATE ATTORNEY GENERAL ENFORCEMENT.—

“(1) IN GENERAL.—

“(A) CIVIL ACTIONS.—In any case in which the attorney general of a State 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 any person in a practice that is prohibited under this section, the State, as *parens patriae*, may bring a civil action on behalf of the residents of the State in a district court of the United States of appropriate jurisdiction to—

“(i) enjoin that practice;

“(ii) enforce compliance with such section;

“(iii) obtain damages, restitution, or other compensation on behalf of residents of the State; or

“(iv) obtain such other relief as the court may consider appropriate.

“(B) NOTICE.—

“(i) IN GENERAL.—Before filing an action under subparagraph (A), the attorney general of the State involved shall provide to the Attorney General—

“(I) written notice of the action; and

“(II) a copy of the complaint for the action.

“(ii) EXEMPTION.—

“(1) IN GENERAL.—Clause (i) shall not apply with respect to the filing of an action by an attorney general of a State under this subsection, 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.—With respect to an action described in subclause (1), the attorney general of a State shall provide notice and a copy of the complaint to the Attorney General at the same time as the State attorney general files the action.

“(2) INTERVENTION.—

“(A) IN GENERAL.—On receiving notice under paragraph (1)(B), the Attorney General shall have the right to intervene in the action that is the subject of the notice.

“(B) EFFECT OF INTERVENTION.—If the Attorney General intervenes in the action under paragraph (1), the Attorney General shall have the right to be heard with respect to any matter that arises in that action.

“(3) CONSTRUCTION.—For purposes of bringing any civil action under paragraph (1), nothing in this section 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—

“(A) conduct investigations;

“(B) administer oaths or affirmations; or

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

“(4) ACTIONS BY THE ATTORNEY GENERAL OF THE UNITED STATES.—In any case in which an action is instituted by or on behalf of the Attorney General for violation of a practice that is prohibited under this section, no State may, during the pendency of that action, institute an action under paragraph (1) against any defendant named in the complaint in that action for violation of that practice.

“(5) VENUE; SERVICE OF PROCESS.—

“(A) VENUE.—Any action brought under paragraph (1) 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 paragraph (1), process may be served in any district in which the defendant—

“(i) is an inhabitant; or

“(ii) may be found.

“(f) SUNSET.—This section shall not apply on or after the date that is 6 years after the effective date of this section.”.

(b) EVALUATION AND REPORT.—Not later than the date that is 6 years and 6 months after the date of enactment of this Act, the Attorney General, in consultation with the chairman of the Federal Trade Commission, shall issue a report evaluating the effectiveness and efficiency of section 1150A of the Social Security Act (as added by subsection (a)) and shall make recommendations to Congress as to any legislative action determined to be necessary or advisable with respect to such section, including a recommendation regarding whether to reauthorize such section.

(c) EFFECTIVE DATE.—The amendment made by subsection (a) shall apply to requests to provide a social security number occurring after the date that is 1 year after the date of enactment of this Act.

**SEC. 207. EXTENSION OF CIVIL MONETARY PENALTIES FOR MISUSE OF A SOCIAL SECURITY NUMBER.**

(a) TREATMENT OF WITHHOLDING OF MATERIAL FACTS.—

(1) CIVIL PENALTIES.—The first sentence of section 1129(a)(1) of the Social Security Act (42 U.S.C. 1320a-8(a)(1)) is amended—

(A) by striking “who” and inserting “who—”;

(B) by striking “makes” and all that follows through “shall be subject to” and inserting the following:

“(A) makes, or causes to be made, a statement or representation of a material fact, for use in determining any initial or continuing right to or the amount of monthly insurance benefits under title II or benefits or payments under title VIII or XVI, that the person knows or should know is false or misleading;

“(B) makes such a statement or representation for such use with knowing disregard for the truth; or

“(C) omits from a statement or representation for such use, or otherwise withholds disclosure of, a fact which the individual knows or should know is material to the determination of any initial or continuing right to or the amount of monthly insurance benefits under title II or benefits or payments under title VIII or XVI and the individual knows, or should know, that the statement or representation with such omission is false or misleading or that the withholding of such disclosure is misleading, shall be subject to”;

(C) by inserting “or each receipt of such benefits while withholding disclosure of such fact” after “each such statement or representation”;

(D) by inserting “or because of such withholding of disclosure of a material fact” after “because of such statement or representation”; and

(E) by inserting “or such a withholding of disclosure” after “such a statement or representation”.

(2) ADMINISTRATIVE PROCEDURE FOR IMPOSING PENALTIES.—The first sentence of section 1129A(a) of the Social Security Act (42 U.S.C. 1320a-8a(a)) is amended—

(A) by striking “who” and inserting “who—”; and

(B) by striking “makes” and all that follows through “shall be subject to” and inserting the following:

“(1) makes, or causes to be made, a statement or representation of a material fact,

for use in determining any initial or continuing right to or the amount of monthly insurance benefits under title II or benefits or payments under title VIII or XVI, that the person knows or should know is false or misleading;

“(2) makes such a statement or representation for such use with knowing disregard for the truth; or

“(3) omits from a statement or representation for such use, or otherwise withholds disclosure of, a fact which the individual knows or should know is material to the determination of any initial or continuing right to or the amount of monthly insurance benefits under title II or benefits or payments under title VIII or XVI and the individual knows, or should know, that the statement or representation with such omission is false or misleading or that the withholding of such disclosure is misleading, shall be subject to”.

(b) APPLICATION OF CIVIL MONEY PENALTIES TO ELEMENTS OF CRIMINAL VIOLATIONS.—Section 1129(a) of the Social Security Act (42 U.S.C. 1320a-8(a)), as amended by subsection (a)(1), is amended—

(1) by redesignating paragraph (2) as paragraph (4);

(2) by redesignating the last sentence of paragraph (1) as paragraph (2) and inserting such paragraph after paragraph (1); and

(3) by inserting after paragraph (2) (as so redesignated) the following:

“(3) Any person (including an organization, agency, or other entity) who—

“(A) uses a social security account number that such person knows or should know has been assigned by the Commissioner of Social Security (in an exercise of authority under section 205(c)(2) to establish and maintain records) on the basis of false information furnished to the Commissioner by any person;

“(B) falsely represents a number to be the social security account number assigned by the Commissioner of Social Security to any individual, when such person knows or should know that such number is not the social security account number assigned by the Commissioner to such individual;

“(C) knowingly alters a social security card issued by the Commissioner of Social Security, or possesses such a card with intent to alter it;

“(D) knowingly displays, sells, or purchases a card that is, or purports to be, a card issued by the Commissioner of Social Security, or possesses such a card with intent to display, purchase, or sell it;

“(E) counterfeits a social security card, or possesses a counterfeit social security card with intent to display, sell, or purchase it;

“(F) discloses, uses, compels the disclosure of, or knowingly displays, sells, or purchases the social security account number of any person in violation of the laws of the United States;

“(G) with intent to deceive the Commissioner of Social Security as to such person's true identity (or the true identity of any other person) furnishes or causes to be furnished false information to the Commissioner with respect to any information required by the Commissioner in connection with the establishment and maintenance of the records provided for in section 205(c)(2);

“(H) offers, for a fee, to acquire for any individual, or to assist in acquiring for any individual, an additional social security account number or a number which purports to be a social security account number; or

“(I) being an officer or employee of a Federal, State, or local agency in possession of any individual's social security account number, willfully acts or fails to act so as to cause a violation by such agency of clause (vi)(II) or (x) of section 205(c)(2)(C),

shall be subject to, in addition to any other penalties that may be prescribed by law, a civil money penalty of not more than \$5,000 for each violation. Such person shall also be subject to an assessment, in lieu of damages sustained by the United States resulting from such violation, of not more than twice the amount of any benefits or payments paid as a result of such violation.”.

(c) CLARIFICATION OF TREATMENT OF RECOVERED AMOUNTS.—Section 1129(e)(2)(B) of the Social Security Act (42 U.S.C. 1320a-8(e)(2)(B)) is amended by striking “In the case of amounts recovered arising out of a determination relating to title VIII or XVI,” and inserting “In the case of any other amounts recovered under this section.”.

(d) CONFORMING AMENDMENTS.—

(1) Section 1129(b)(3)(A) of the Social Security Act (42 U.S.C. 1320a-8(b)(3)(A)) is amended by striking “charging fraud or false statements”.

(2) Section 1129(c)(1) of the Social Security Act (42 U.S.C. 1320a-8(c)(1)) is amended by striking “and representations” and inserting “, representations, or actions”.

(3) Section 1129(e)(1)(A) of the Social Security Act (42 U.S.C. 1320a-8(e)(1)(A)) is amended by striking “statement or representation referred to in subsection (a) was made” and inserting “violation occurred”.

(e) EFFECTIVE DATES.—

(1) IN GENERAL.—Except as provided in paragraph (2), the amendments made by this section shall apply with respect to violations of sections 1129 and 1129A of the Social Security Act (42 U.S.C. 1320-8 and 1320a-8a), as amended by this section, committed after the date of enactment of this Act.

(2) VIOLATIONS BY GOVERNMENT AGENTS IN POSSESSION OF SOCIAL SECURITY NUMBERS.—Section 1129(a)(3)(I) of the Social Security Act (42 U.S.C. 1320a-8(a)(3)(I)), as added by subsection (b), shall apply with respect to violations of that section occurring on or after the effective date described in section 202(c).

**SEC. 208. CRIMINAL PENALTIES FOR THE MISUSE OF A SOCIAL SECURITY NUMBER.**

(a) PROHIBITION OF WRONGFUL USE AS PERSONAL IDENTIFICATION NUMBER.—No person may obtain any individual's social security number for purposes of locating or identifying an individual with the intent to physically injure, harm, or use the identity of the individual for any illegal purpose.

(b) CRIMINAL SANCTIONS.—Section 208(a) of the Social Security Act (42 U.S.C. 408(a)) is amended—

(1) in paragraph (8), by inserting “or” after the semicolon; and

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

“(9) except as provided in subsections (e) and (f) of section 1028A of title 18, United States Code, knowingly and willfully displays, sells, or purchases (as those terms are defined in section 1028A(a) of title 18, United States Code) any individual's social security account number without having met the prerequisites for consent under section 1028A(d) of title 18, United States Code; or

“(10) obtains any individual's social security number for the purpose of locating or identifying the individual with the intent to injure or to harm that individual, or to use the identity of that individual for an illegal purpose.”.

**SEC. 209. CIVIL ACTIONS AND CIVIL PENALTIES.**

(a) CIVIL ACTION IN STATE COURTS.—

(1) IN GENERAL.—Any individual aggrieved by an act of any person in violation of this title or any amendments made by this title may, if otherwise permitted by the laws or rules of the court of a State, bring in an appropriate court of that State—

(A) an action to enjoin such violation;

(B) an action to recover for actual monetary loss from such a violation, or to receive up to \$500 in damages for each such violation, whichever is greater; or

(C) both such actions.

It shall be an affirmative defense in any action brought under this paragraph that the defendant has established and implemented, with due care, reasonable practices and procedures to effectively prevent violations of the regulations prescribed under this title. If the court finds that the defendant willfully or knowingly violated the regulations prescribed under this subsection, the court may, in its discretion, increase the amount of the award to an amount equal to not more than 3 times the amount available under subparagraph (B).

(2) **STATUTE OF LIMITATIONS.**—An action may be commenced under this subsection not later than the earlier of—

(A) 5 years after the date on which the alleged violation occurred; or

(B) 3 years after the date on which the alleged violation was or should have been reasonably discovered by the aggrieved individual.

(3) **NONEXCLUSIVE REMEDY.**—The remedy provided under this subsection shall be in addition to any other remedies available to the individual.

(b) **CIVIL PENALTIES.**—

(1) **IN GENERAL.**—Any person who the Attorney General determines has violated any section of this title or of any amendments made by this title shall be subject, in addition to any other penalties that may be prescribed by law—

(A) to a civil penalty of not more than \$5,000 for each such violation; and

(B) to a civil penalty of not more than \$50,000, if the violations have occurred with such frequency as to constitute a general business practice.

(2) **DETERMINATION OF VIOLATIONS.**—Any willful violation committed contemporaneously with respect to the social security numbers of 2 or more individuals by means of mail, telecommunication, or otherwise, shall be treated as a separate violation with respect to each such individual.

(3) **ENFORCEMENT PROCEDURES.**—The provisions of section 1128A of the Social Security Act (42 U.S.C. 1320a-7a), other than subsections (a), (b), (f), (h), (i), (j), (m), and (n) and the first sentence of subsection (c) of such section, and the provisions of subsections (d) and (e) of section 205 of such Act (42 U.S.C. 405) shall apply to a civil penalty action under this subsection in the same manner as such provisions apply to a penalty or proceeding under section 1128A(a) of such Act (42 U.S.C. 1320a-7a(a)), except that, for purposes of this paragraph, any reference in section 1128A of such Act (42 U.S.C. 1320a-7a) to the Secretary shall be deemed to be a reference to the Attorney General.

#### **SEC. 210. FEDERAL INJUNCTIVE AUTHORITY.**

In addition to any other enforcement authority conferred under this title or the amendments made by this title, the Federal Government shall have injunctive authority with respect to any violation by a public entity of any provision of this title or of any amendments made by this title.

### **TITLE III—LIMITATIONS ON SALE AND SHARING OF NONPUBLIC PERSONAL FINANCIAL INFORMATION**

#### **SEC. 301. DEFINITION OF SALE.**

Section 509 of the Gramm-Leach-Bliley Act (15 U.S.C. 6809) is amended by adding at the end the following:

“(12) **SALE.**—The terms ‘sale’, ‘sell’, and ‘sold’, with respect to nonpublic personal information, mean the exchange of such information for any thing of value, directly or in-

directly, including the licensing, bartering, or renting of such information.”.

#### **SEC. 302. RULES APPLICABLE TO SALE OF NON-PUBLIC PERSONAL INFORMATION.**

Section 502 of the Gramm-Leach-Bliley Act (15 U.S.C. 6802) is amended—

(1) in the section heading, by inserting “**SALES, AND OTHER SHARING**” after “**DISCLOSURES**”;

(2) in subsection (a), by striking “disclose to” and inserting “sell or otherwise disclose to an affiliate or”;

(3) in subsection (b)—

(A) in the subsection heading, by inserting “**FOR DISCLOSURES TO AFFILIATES**” before the period;

(B) by striking “a nonaffiliated third party” each place that term appears and inserting “an affiliate”;

(C) by striking “such third party” each place that term appears and inserting “such affiliate”;

(D) by striking “may not disclose” and inserting “may not sell or otherwise disclose”;

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

“(2) **EXCEPTION.**—This subsection shall not prevent a financial institution from providing nonpublic personal information to an affiliated third party to perform services for or functions on behalf of the financial institution, including marketing of the financial institution’s own products or services, if the financial institution fully discloses the provision of such information and requires the affiliate to maintain the confidentiality of such information.”;

(4) in subsection (d), by striking “disclose” and inserting “sell or otherwise disclose”;

(5) by striking subsection (e);

(6) by redesignating subsections (c) and (d) as subsections (e) and (f), respectively; and

(7) by inserting after subsection (b) the following:

“(c) **OPT IN FOR DISCLOSURES TO NON-AFFILIATED THIRD PARTIES.**—

“(1) **AFFIRMATIVE CONSENT REQUIRED.**—A financial institution may not sell or otherwise disclose nonpublic personal information to any nonaffiliated third party, unless the consumer to whom the information pertains—

“(A) has affirmatively consented to the sale or disclosure of such information; and

“(B) has not withdrawn the consent.

“(2) **EXCEPTION.**—This subsection shall not prevent a financial institution from providing nonpublic personal information to a nonaffiliated third party to perform services for or functions on behalf of the financial institution, including marketing of the financial institution’s own products or services (subject to subsection (d) with respect to joint agreements between 2 or more financial institutions), if the financial institution fully discloses the provision of such information and enters into a contractual agreement with the nonaffiliated third party that requires that third party to maintain the confidentiality of such information.

“(d) **OPT OUT FOR JOINT AGREEMENTS.**—A financial institution may not sell or otherwise disclose nonpublic personal information to a nonaffiliated third party for the purpose of offering financial products or services pursuant to a joint agreement between 2 or more financial institutions, unless—

“(1) the financial institution clearly and conspicuously discloses to the consumer to whom the information pertains, in writing or in electronic form or other form permitted by the regulations prescribed under section 504, that such information may be disclosed to such nonaffiliated third party;

“(2) the consumer is given the opportunity, before the time that such information is initially disclosed, to direct that such informa-

tion not be disclosed to such nonaffiliated third party;

“(3) the consumer is given an explanation of how the consumer can exercise that non-disclosure option; and

“(4) the financial institution receiving the nonpublic personal information signs a written agreement obliging it—

“(A) to maintain the confidentiality of the information; and

“(B) to refrain from using, selling, or otherwise disclosing the information other than to carry out the joint offering or servicing of the financial product or financial service that is the subject of the written agreement.”.

#### **SEC. 303. EXCEPTIONS TO DISCLOSURE PROHIBITION.**

(a) **IN GENERAL.**—Section 502 of the Gramm-Leach-Bliley Act (15 U.S.C. 6802), as amended by this title, is amended by adding at the end the following:

“(g) **GENERAL EXCEPTIONS.**—Notwithstanding any other provision of this section, this section does not prohibit—

“(1) the sale or other disclosure of nonpublic personal information to an affiliate or a nonaffiliated third party—

“(A) as necessary to effect, administer, or enforce a transaction requested or authorized by the consumer to whom the information pertains, or in connection with—

“(i) servicing or processing a financial product or service requested or authorized by the consumer;

“(ii) maintaining or servicing the account of the consumer with the financial institution, or with another entity as part of a private label credit card program or other extension of credit on behalf of such entity; or

“(iii) a proposed or actual securitization, secondary market sale (including sales of servicing rights), or similar transaction related to a transaction of the consumer;

“(B) with the consent or at the direction of the consumer, in accordance with applicable rules prescribed under this subtitle;

“(C) to the extent specifically permitted or required under other provisions of law and in accordance with the Right to Financial Privacy Act of 1978; or

“(D) to law enforcement agencies (including a Federal functional regulator, the Secretary of the Treasury, with respect to subchapter II of chapter 53 of title 31, United States Code, and chapter 2 of title I of Public Law 91-508 (12 U.S.C. 1951-1959), a State insurance authority, or the Federal Trade Commission), self-regulatory organizations, or for an investigation on a matter related to public safety;

“(2) the disclosure, other than the sale, of nonpublic personal information to identify or locate missing and abducted children, witnesses, criminals, and fugitives, parties to lawsuits, parents, delinquents in child support payments, organ and bone marrow donors, pension fund beneficiaries, and missing heirs; or

“(3) the disclosure, other than the sale, of nonpublic personal information—

“(A) to protect the confidentiality or security of the records of the financial institution pertaining to the consumer, the service or product, or the transaction therein;

“(B) to protect against or prevent actual or potential fraud, unauthorized transactions, claims, or other liability;

“(C) for required institutional risk control, or for resolving customer disputes or inquiries;

“(D) to persons holding a legal or beneficial interest relating to the consumer;

“(E) to persons acting in a fiduciary or representative capacity on behalf of the consumer;

“(F) to provide information to insurance rate advisory organizations, guaranty funds

or agencies, applicable rating agencies of the financial institution, persons assessing the compliance of the institution with industry standards, or the attorneys, accountants, or auditors of the institution;

“(G) to a consumer reporting agency, in accordance with the Fair Credit Reporting Act or from a consumer report reported by a consumer reporting agency, as those terms are defined in that Act;

“(H) in connection with a proposed or actual sale, merger, transfer, or exchange of all or a portion of a business or operating unit if the disclosure of nonpublic personal information concerns solely consumers of such business or unit;

“(I) to comply with Federal, State, or local laws, rules, or other applicable legal requirements, or with a properly authorized civil, criminal, or regulatory investigation or subpoena or summons by Federal, State, or local authorities; or

“(J) to respond to judicial process or government regulatory authorities having jurisdiction over the financial institution for examination, compliance, or other purposes, as authorized by law.

“(h) DENIAL OF SERVICE PROHIBITED.—A financial institution may not deny any consumer a financial product or a financial service as a result of the refusal by the consumer to grant consent to disclosure under this section or the exercise by the consumer of a nondisclosure option under this section, except that nothing in this subsection may be construed to prohibit a financial institution from offering incentives to elicit consumer consent to the use of his or her nonpublic personal information.”.

(b) REPEAL OF REGULATORY EXEMPTION AUTHORITY.—Section 504 of the Gramm-Leach-Bliley Act (15 U.S.C. 6804) is amended—

(1) by striking subsection (b);

(2) by striking “(a) REGULATORY AUTHORITY.—”;

(3) by redesignating paragraphs (1), (2), and (3) as subsections (a), (b), and (c), respectively, and moving the margins 2 ems to the left; and

(4) by striking “paragraph (1)” and inserting “subsection (a)”.

#### SEC. 304. CONFORMING AMENDMENTS.

Title V of the Gramm-Leach-Bliley Act (15 U.S.C. 6801 et seq.) is amended—

(1) in section 503(b)(1) (15 U.S.C. 6803(b)(1))—

(A) by inserting “affiliates and” before “nonaffiliated”; and

(B) in subparagraph (A), by striking “502(e)” and inserting “502(g)”; and

(2) in section 509(3)(D) (15 U.S.C. 6809(3)(D)), by striking “502(e)(1)(C)” and inserting “502(g)(1)(A)(iii)”.

#### SEC. 305. REGULATORY AUTHORITY.

Not later than 6 months after the date of enactment of this Act, the agencies referred to in section 504(a)(1) of the Gramm-Leach-Bliley Act (15 U.S.C. 6804(a)(1)) shall promulgate final regulations in accordance with that section 504 to carry out the amendments made by this Act.

#### SEC. 306. EFFECTIVE DATE.

This title and the amendments made by this title shall take effect 6 months after the date of enactment of this Act.

### TITLE IV—LIMITATIONS ON THE PROVISION OF PROTECTED HEALTH INFORMATION

#### SEC. 401. DEFINITIONS.

In this title:

(1) BUSINESS ASSOCIATE.—

(A) IN GENERAL.—Except as provided in subparagraph (B), the term “business associate” means, with respect to a covered entity, a person who—

(i) on behalf of such covered entity or of an organized health care arrangement in which

the covered entity participates, but other than in the capacity of a member of the workforce of such covered entity or arrangement, performs, or assists in the performance of—

(I) a function or activity involving the use or disclosure of individually identifiable health information, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing, benefit management, practice management, and repricing; or

(II) any other function or activity regulated under subchapter C of title 45, Code of Federal Regulations; or

(ii) provides, other than in the capacity of a member of the workforce of such covered entity, legal, actuarial, accounting, consulting, data aggregation (as defined in section 164.501 of title 45, Code of Federal Regulations), management, administrative, accreditation, or financial services to or for such covered entity, or to or for an organized health care arrangement in which the covered entity participates, where the provision of the service involves the disclosure of individually identifiable health information from such covered entity or arrangement, or from another business associate of such covered entity or arrangement, to the person.

(B) LIMITATIONS.—

(i) IN GENERAL.—A covered entity participating in an organized health care arrangement that performs a function or activity as described by subparagraph (A)(i) for or on behalf of such organized health care arrangement, or that provides a service as described in subparagraph (A)(ii) to or for such organized health care arrangement, does not, simply through the performance of such function or activity or the provision of such service, become a business associate of other covered entities participating in such organized health care arrangement.

(ii) LIMITATION.—A covered entity may be a business associate of another covered entity.

(2) COVERED ENTITY.—The term “covered entity” means—

(A) a health plan;

(B) a health care clearinghouse; and

(C) a health care provider who transmits any health information in electronic form in connection with a transaction covered by parts 160 through 164 of title 45, Code of Federal Regulations.

(3) DISCLOSURE.—The term “disclosure” means the release, transfer, provision of access to, or divulging in any other manner of information outside the entity holding the information.

(4) EMPLOYER.—The term “employer” has the meaning given that term in section 3401(d) of the Internal Revenue Code of 1986.

(5) GROUP HEALTH PLAN.—The term “group health plan” means an employee welfare benefit plan (as defined in section 3(1) of the Employee Retirement Income and Security Act of 1974 (29 U.S.C. 1002(1)), including insured and self-insured plans, to the extent that the plan provides medical care (as defined in section 2791(a)(2) of the Public Health Service Act, 42 U.S.C. 300gg-91(a)(2)), including items and services paid for as medical care, to employees or their dependents directly or through insurance, reimbursement, or otherwise, that—

(A) has 50 or more participants (as defined in section 3(7) of Employee Retirement Income and Security Act of 1974, 29 U.S.C. 1002(7)); or

(B) is administered by an entity other than the employer that established and maintains the plan.

(6) HEALTH CARE.—The term “health care” includes, but is not limited to, the following:

(A) Preventive, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care

and counseling, service, assessment, or procedure with respect to the physical or mental condition, or functional status, of an individual or that affects the structure or function of the body.

(B) The sale or dispensing of a drug, device, equipment, or other item in accordance with a prescription.

(7) HEALTH CARE CLEARINGHOUSE.—The term “health care clearinghouse” means a public or private entity, including a billing service, repricing company, community health management information system or community health information system, and value-added networks and switches, that—

(A) processes or facilitates the processing of health information received from another entity in a nonstandard format or containing nonstandard data content into standard data elements or a standard transaction; or

(B) receives a standard transaction from another entity and processes or facilitates the processing of health information into nonstandard format or nonstandard data content for the receiving entity.

(8) HEALTH CARE PROVIDER.—The term “health care provider” has the meaning given the terms “provider of services” and “provider of medical or health services” in subsections (u) and (s) of section 1861 of the Social Security Act (42 U.S.C. 1395x), respectively, and includes any other person or organization who furnishes, bills, or is paid for health care in the normal course of business.

(9) HEALTH INFORMATION.—The term “health information” means any information, whether oral or recorded in any form or medium, that—

(A) is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and

(B) relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual.

(10) HEALTH INSURANCE ISSUER.—The term “health insurance issuer” means a health insurance issuer (as defined in section 2791(b)(2) of the Public Health Service Act, 42 U.S.C. 300gg-91(b)(2)) and used in the definition of health plan in this section and includes an insurance company, insurance service, or insurance organization (including an HMO) that is licensed to engage in the business of insurance in a State and is subject to State law that regulates insurance. Such term does not include a group health plan.

(11) HEALTH MAINTENANCE ORGANIZATION.—The term “health maintenance organization” (HMO) (as defined in section 2791(b)(3) of the Public Health Service Act, 42 U.S.C. 300gg-91(b)(3)) and used in the definition of health plan in this section, means a federally qualified HMO, an organization recognized as an HMO under State law, or a similar organization regulated for solvency under State law in the same manner and to the same extent as such an HMO.

(12) HEALTH OVERSIGHT AGENCY.—The term “health oversight agency” means an agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, or a person or entity acting under a grant of authority from or contract with such public agency, including the employees or agents of such public agency or its contractors or persons or entities to whom it has granted authority, that is authorized by law to oversee the health care system (whether public or private) or government programs in which health information is necessary to determine eligibility or compliance, or to enforce civil

rights laws for which health information is relevant.

(13) HEALTH PLAN.—The term “health plan” means an individual or group plan that provides, or pays the cost of, medical care, as defined in section 2791(a)(2) of the Public Health Service Act (42 U.S.C. 300gg-91(a)(2))—

(A) including, singly or in combination—

- (i) a group health plan;
- (ii) a health insurance issuer;
- (iii) an HMO;
- (iv) part A or B of the medicare program under title XVIII of the Social Security Act (42 U.S.C. 1395 et seq.);
- (v) the medicaid program under title XIX of the Social Security Act (42 U.S.C. 1396 et seq.);
- (vi) an issuer of a medicare supplemental policy (as defined in section 1882(g)(1) of the Social Security Act, 42 U.S.C. 1395ss(g)(1));
- (vii) an issuer of a long-term care policy, excluding a nursing home fixed-indemnity policy;
- (viii) an employee welfare benefit plan or any other arrangement that is established or maintained for the purpose of offering or providing health benefits to the employees of 2 or more employers;
- (ix) the health care program for active military personnel under title 10, United States Code;
- (x) the veterans health care program under chapter 17 of title 38, United States Code;
- (xi) the Civilian Health and Medical Program of the Uniformed Services (CHAMPUS) (as defined in section 1072(4) of title 10, United States Code);
- (xii) the Indian Health Service program under the Indian Health Care Improvement Act (25 U.S.C. 1601 et seq.);
- (xiii) the Federal Employees Health Benefits Program under chapter 89 of title 5, United States Code;
- (xiv) an approved State child health plan under title XXI of the Social Security Act (42 U.S.C. 1397aa et seq.), providing benefits for child health assistance that meet the requirements of section 2103 of such Act (42 U.S.C. 1397cc);
- (xv) the Medicare+Choice program under part C of title XVIII of the Social Security Act (42 U.S.C. 1395w-21 et seq.);
- (xvi) a high risk pool that is a mechanism established under State law to provide health insurance coverage or comparable coverage to eligible individuals; and
- (xvii) any other individual or group plan, or combination of individual or group plans, that provides or pays for the cost of medical care (as defined in section 2791(a)(2) of the Public Health Service Act (42 U.S.C. 300gg-91(a)(2))); and

(B) excluding—

(i) any policy, plan, or program to the extent that it provides, or pays for the cost of, excepted benefits that are listed in section 2791(c)(1) of the Public Health Service Act (42 U.S.C. 300gg-91(c)(1)); and

(ii) a government-funded program (other than 1 listed in clause (i) through (xvi) of subparagraph (A)), whose principal purpose is other than providing, or paying the cost of, health care, or whose principal activity is the direct provision of health care to persons, or the making of grants to fund the direct provision of health care to persons.

(14) INDIVIDUALLY IDENTIFIABLE HEALTH INFORMATION.—The term “individually identifiable health information” means information that is a subset of health information, including demographic information collected from an individual, that—

(A) is created or received by a covered entity or employer; and

(B)(i) relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an

individual, or the past, present, or future payment for the provision of health care to an individual; and

(ii)(I) identifies an individual; or

(II) with respect to which there is a reasonable basis to believe that the information can be used to identify an individual.

(15) LAW ENFORCEMENT OFFICIAL.—The term “law enforcement official” means an officer or employee of any agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, who is empowered by law to—

(A) investigate or conduct an official inquiry into a potential violation of law; or

(B) prosecute or otherwise conduct a criminal, civil, or administrative proceeding arising from an alleged violation of law.

(16) LIFE INSURER.—The term “life insurer” means a life insurance company (as defined in section 816 of the Internal Revenue Code of 1986), including the employees and agents of such company.

(17) MARKETING.—The term “marketing” means to make a communication about a product or service that encourages recipients of the communication to purchase or use the product or service.

(18) NONCOVERED ENTITY.—The term “non-covered entity” means any person or public or private entity that is not a covered entity, including but not limited to a business associate of a covered entity, a covered entity if such covered entity is acting as a business associate, a health researcher, school or university, life insurer, employer, public health authority, health oversight agency, or law enforcement official, or any person acting as an agent of such entities or persons.

(19) ORGANIZED HEALTH CARE ARRANGEMENT.—The term “organized health care arrangement” means—

(A) a clinically integrated care setting in which individuals typically receive health care from more than 1 health care provider;

(B) an organized system of health care in which more than 1 covered entity participates, and in which the participating covered entities—

(i) hold themselves out to the public as participating in a joint arrangement; and

(ii) participate in joint activities including at least—

(I) utilization review, in which health care decisions by participating covered entities are reviewed by other participating covered entities or by a third party on their behalf;

(II) quality assessment and improvement activities, in which treatment provided by participating covered entities is assessed by other participating covered entities or by a third party on their behalf; or

(III) payment activities, if the financial risk for delivering health care is shared, in part or in whole, by participating covered entities through the joint arrangement and if protected health information created or received by a covered entity is reviewed by other participating covered entities or by a third party on their behalf for the purpose of administering the sharing of financial risk;

(C) a group health plan and a health insurance issuer or HMO with respect to such group health plan, but only with respect to protected health information created or received by such health insurance issuer or HMO that relates to individuals who are or who have been participants or beneficiaries in such group health plan;

(D) a group health plan and 1 or more other group health plans each of which are maintained by the same plan sponsor; or

(E) the group health plans described in subparagraph (D) and health insurance issuers or HMOs with respect to such group health plans, but only with respect to protected

health information created or received by such health insurance issuers or HMOs that relates to individuals who are or have been participants or beneficiaries in any of such group health plans.

(20) PROTECTED HEALTH INFORMATION.—

(A) IN GENERAL.—The term “protected health information” means individually identifiable health information that, except as provided in subparagraph (B), is—

(i) transmitted by electronic media;

(ii) maintained in any medium described in the definition of electronic media in section 162.103 of title 45, Code of Federal Regulations; or

(iii) transmitted or maintained in any other form or medium.

(B) EXCLUSIONS.—Such term does not include individually identifiable health information—

(i) education records covered by the Family Educational Rights and Privacy Act of 1974 (section 444 of the General Education Provisions Act (20 U.S.C. 1232g));

(ii) records described in subsection (a)(4)(B)(iv) of that Act; or

(iii) employment records held by a covered entity in its role as an employer.

(21) PUBLIC HEALTH AUTHORITY.—The term “public health authority” means an agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, or a person or entity acting under a grant of authority from or contract with such public agency, including employees or agents of such public agency or its contractors or persons or entities to whom it has granted authority, that is responsible for public health matters as part of its official mandate.

(22) SCHOOL OR UNIVERSITY.—The term “school or university” means an institution or place for instruction or education, including an elementary school, secondary school, or institution of higher learning, a college, or an assemblage of colleges united under 1 corporate organization or government.

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

(24) SALE; SELL; SOLD.—The terms “sale”, “sell”, and “sold”, with respect to protected health information, mean the exchange of such information for anything of value, directly or indirectly, including the licensing, bartering, or renting of such information.

(25) USE.—The term “use” means, with respect to individually identifiable health information, the sharing, employment, application, utilization, examination, or analysis of such information within an entity that maintains such information.

(26) WRITING.—The term “writing” means writing in either a paper-based or computer-based form, including electronic and digital signatures.

#### SEC. 402. PROHIBITION AGAINST SELLING PROTECTED HEALTH INFORMATION.

(a) VALID AUTHORIZATION REQUIRED.—

(1) IN GENERAL.—A noncovered entity shall not sell the protected health information of an individual or use such information for marketing purposes without an authorization that is valid under section 403. When a noncovered entity obtains or receives authorization to sell such information, such sale must be consistent with such authorization.

(2) NO DUPLICATE AUTHORIZATION REQUIRED.—Nothing in paragraph (1) shall be construed as requiring a noncovered entity that receives from a covered entity an authorization that is valid under section 403 to obtain a separate authorization from an individual before the sale or use of the individual's protected health information so long as the sale or use of the information is consistent with the terms of the authorization.

(b) SCOPE.—A sale of protected health information as described under subsection (a) shall be limited to the minimum amount of information necessary to accomplish the purpose for which the sale is made.

(c) PURPOSE.—A recipient of information sold pursuant to this title may use or disclose such information solely to carry out the purpose for which the information was sold.

(d) NOT REQUIRED.—Nothing in this title permitting the sale of protected health information shall be construed to require such sale.

(e) IDENTIFICATION OF INFORMATION AS PROTECTED HEALTH INFORMATION.—Information sold pursuant to this title shall be clearly identified as protected health information.

(f) NO WAIVER.—Except as provided in this title, an individual's authorization to sell protected health information shall not be construed as a waiver of any rights that the individual has under other Federal or State laws, the rules of evidence, or common law.

**SEC. 403. AUTHORIZATION FOR SALE OR MARKETING OF PROTECTED HEALTH INFORMATION BY NONCOVERED ENTITIES.**

(a) VALID AUTHORIZATION.—A valid authorization is a document that complies with all requirements of this section. Such authorization may include additional information not required under this section, provided that such information is not inconsistent with the requirements of this section.

(b) DEFECTIVE AUTHORIZATION.—An authorization is not valid, if the document submitted has any of the following defects:

(1) The expiration date has passed or the expiration event is known by the noncovered entity to have occurred.

(2) The authorization has not been filled out completely, with respect to an element described in subsections (e) and (f).

(3) The authorization is known by the noncovered entity to have been revoked.

(4) The authorization lacks an element required by subsections (e) and (f).

(5) Any material information in the authorization is known by the noncovered entity to be false.

(c) REVOCATION OF AUTHORIZATION.—An individual may revoke an authorization provided under this section at any time provided that the revocation is in writing, except to the extent that the noncovered entity has taken action in reliance thereon.

(d) DOCUMENTATION.—

(1) IN GENERAL.—A noncovered entity must document and retain any signed authorization under this section as required under paragraph (2).

(2) STANDARD.—A noncovered entity shall, if a communication is required by this title to be in writing, maintain such writing, or an electronic copy, as documentation.

(3) RETENTION PERIOD.—A noncovered entity shall retain the documentation required by this section for 6 years from the date of its creation or the date when it last was in effect, whichever is later.

(e) CONTENT OF AUTHORIZATION.—

(1) CONTENT.—An authorization described in subsection (a) shall—

(A) contain a description of the information to be sold that identifies such information in a specific and meaningful manner;

(B) contain the name or other specific identification of the person, or class of persons, authorized to sell the information;

(C) contain the name or other specific identification of the person, or class of persons, to whom the information is to be sold;

(D) include an expiration date or an expiration event relating to the selling of such information that signifies that the authorization is valid until such date or event;

(E) include a statement that the individual has a right to revoke the authorization in

writing and the exceptions to the right to revoke, and a description of the procedure involved in such revocation;

(F) be in writing and include the signature of the individual and the date, or if the authorization is signed by a personal representative of the individual, a description of such representative's authority to act for the individual; and

(G) include a statement explaining the purpose for which such information is sold.

(2) PLAIN LANGUAGE.—The authorization shall be written in plain language.

(f) NOTICE.—

(1) IN GENERAL.—The authorization shall include a statement that the individual may—

(A) inspect or copy the protected health information to be sold; and

(B) refuse to sign the authorization.

(2) COPY TO THE INDIVIDUAL.—A noncovered entity shall provide the individual with a copy of the signed authorization.

(g) MODEL AUTHORIZATIONS.—The Secretary, after notice and opportunity for public comment, shall develop and disseminate model written authorizations of the type described in this section and model statements of the limitations on such authorizations. Any authorization obtained on a model authorization form developed by the Secretary pursuant to the preceding sentence shall be deemed to satisfy the requirements of this section.

(h) NONCOERCION.—A covered entity or noncovered entity shall not condition the purchase of a product or the provision of a service to an individual based on whether such individual provides an authorization to such entity as described in this section.

**SEC. 404. PROHIBITION AGAINST RETALIATION.**

A noncovered entity that collects protected health information, may not adversely affect another person, directly or indirectly, because such person has exercised a right under this title, disclosed information relating to a possible violation of this title, or associated with, or assisted, a person in the exercise of a right under this title.

**SEC. 405. RULE OF CONSTRUCTION.**

The requirements of this title shall not be construed to impose any additional requirements or in any way alter the requirements imposed upon covered entities under parts 160 through 164 of title 45, Code of Federal Regulations.

**SEC. 406. REGULATIONS.**

(a) IN GENERAL.—The Secretary shall promulgate regulations implementing the provisions of this title.

(b) TIMEFRAME.—Not later than 1 year after the date of enactment of this Act, the Secretary shall publish proposed regulations in the Federal Register. With regard to such proposed regulations, the Secretary shall provide an opportunity for submission of comments by interested persons during a period of not less than 90 days. Not later than 2 years after the date of enactment of this Act, the Secretary shall publish final regulations in the Federal Register.

**SEC. 407. ENFORCEMENT.**

(a) IN GENERAL.—A covered entity or noncovered entity that knowingly violates section 402 shall be subject to a civil money penalty under this section.

(b) AMOUNT.—The civil money penalty described in subsection (a) shall not exceed \$100,000. In determining the amount of any penalty to be assessed, the Secretary shall take into account the previous record of compliance of the entity being assessed with the applicable provisions of this title and the gravity of the violation.

(c) ADMINISTRATIVE REVIEW.—

(1) OPPORTUNITY FOR HEARING.—The entity assessed shall be afforded an opportunity for

a hearing by the Secretary upon request made within 30 days after the date of the issuance of a notice of assessment. In such hearing the decision shall be made on the record pursuant to section 554 of title 5, United States Code. If no hearing is requested, the assessment shall constitute a final and unappealable order.

(2) HEARING PROCEDURE.—If a hearing is requested, the initial agency decision shall be made by an administrative law judge, and such decision shall become the final order unless the Secretary modifies or vacates the decision. Notice of intent to modify or vacate the decision of the administrative law judge shall be issued to the parties within 30 days after the date of the decision of the judge. A final order which takes effect under this paragraph shall be subject to review only as provided under subsection (d).

(d) JUDICIAL REVIEW.—

(1) FILING OF ACTION FOR REVIEW.—Any entity against whom an order imposing a civil money penalty has been entered after an agency hearing under this section may obtain review by the United States district court for any district in which such entity is located or the United States District Court for the District of Columbia by filing a notice of appeal in such court within 30 days from the date of such order, and simultaneously sending a copy of such notice by registered mail to the Secretary.

(2) CERTIFICATION OF ADMINISTRATIVE RECORD.—The Secretary shall promptly certify and file in such court the record upon which the penalty was imposed.

(3) STANDARD FOR REVIEW.—The findings of the Secretary shall be set aside only if found to be unsupported by substantial evidence as provided by section 706(2)(E) of title 5, United States Code.

(4) APPEAL.—Any final decision, order, or judgment of the district court concerning such review shall be subject to appeal as provided in chapter 83 of title 28 of such Code.

(e) FAILURE TO PAY ASSESSMENT; MAINTENANCE OF ACTION.—

(1) FAILURE TO PAY ASSESSMENT.—If any entity fails to pay an assessment after it has become a final and unappealable order, or after the court has entered final judgment in favor of the Secretary, the Secretary shall refer the matter to the Attorney General who shall recover the amount assessed by action in the appropriate United States district court.

(2) NONREVIEWABILITY.—In such action the validity and appropriateness of the final order imposing the penalty shall not be subject to review.

(f) PAYMENT OF PENALTIES.—Except as otherwise provided, penalties collected under this section shall be paid to the Secretary (or other officer) imposing the penalty and shall be available without appropriation and until expended for the purpose of enforcing the provisions with respect to which the penalty was imposed.

**TITLE V—DRIVER'S LICENSE PRIVACY**

**SEC. 501. DRIVER'S LICENSE PRIVACY.**

Section 2725 of title 18, United States Code, is amended by striking paragraphs (2) through (4) and adding the following:

“(2) ‘person’ means an individual, organization, or entity, but does not include a State or agency thereof;

“(3) ‘personal information’ means information that identifies an individual, including an individual's photograph, social security number, driver identification number, name, address (but not the 5-digit zip code), telephone number, medical or disability information, any physical copy of a driver's license, birth date, information on physical characteristics, including height, weight, sex or eye color, or any biometric identifiers on

a license, including a finger print, but not information on vehicular accidents, driving violations, and driver's status;

"(4) 'highly restricted personal information' means an individual's photograph or image, social security number, medical or disability information, any physical copy of a driver's license, driver identification number, birth date, information on physical characteristics, including height, weight, sex, or eye color, or any biometric identifiers on a license, including a finger print; and".

#### TITLE VI—MISCELLANEOUS

##### SEC. 601. ENFORCEMENT BY STATE ATTORNEYS GENERAL.

(a) IN GENERAL.—

(1) CIVIL ACTIONS.—In any case in which the attorney general of a State 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 any person in a practice that is prohibited under title I, II, or IV of this Act or under any amendment made by such a title, the State, as *parens patriae*, may bring a civil action on behalf of the residents of the State in a district court of the United States of appropriate jurisdiction to—

- (A) enjoin that practice;
- (B) enforce compliance with such titles or such amendments;
- (C) obtain damage, restitution, or other compensation on behalf of residents of the State; or
- (D) obtain such other relief as the court may consider to be appropriate.

(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—

- (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 subsection, 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 same time as the State attorney general files the action.

(b) INTERVENTION.—

(1) IN GENERAL.—On receiving notice under subsection (a)(2), the Attorney General shall have the right to intervene in the action that is the subject of the notice.

(2) EFFECT OF INTERVENTION.—If the Attorney General intervenes in an action under subsection (a), the Attorney General shall have the right to be heard with respect to any matter that arises in that action.

(c) CONSTRUCTION.—For purposes of bringing any civil action under subsection (a), nothing in this Act 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.

(d) ACTIONS BY THE ATTORNEY GENERAL OF THE UNITED STATES.—In any case in which an action is instituted by or on behalf of the Attorney General for violation of a practice that is prohibited under title I, II, IV, or V of this Act or under any amendment made by such a title, no State may, during the pendency of that action, institute an action under subsection (a) against any defendant

named in the complaint in that action for violation of that practice.

(e) VENUE; SERVICE OF PROCESS.—

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

(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.

##### SEC. 602. FEDERAL INJUNCTIVE AUTHORITY.

In addition to any other enforcement authority conferred under this Act or under an amendment made by this Act, the Federal Government shall have injunctive authority with respect to any violation of any provision of title I, II, or IV of this Act or of any amendment made by such a title, without regard to whether a public or private entity violates such provision.

By Mrs. FEINSTEIN (for herself and Mr. KYL):

S. 746. A bill to prevent and respond to terrorism and crime at or through ports; to the Committee on Commerce, Science, and Transportation.

Mrs. FEINSTEIN. Mr. President, I rise today to introduce the Anti-Terrorism and Port Security Act of 2003, comprehensive legislation aimed at preventing and punishing a terrorist attack at or through one of our nation's 361 seaports. I would like to thank Senator KYL for joining me in sponsoring this bill.

Currently, our seaports are the gaping hole in our nation's defense against terrorism. According to the U.S. Bureau of Transportation Statistics, about 13 million containers, twenty-foot equivalent units, came into United States ports in 2002.

However, the U.S. government inspected only about two or three percent of these containers—they rest were simply waved through. In addition, in almost every case, these inspections occurred after the containers arrive in the United States.

The problem is that a single container could contain 60,000 pounds of explosives—10 to 15 times the amount in the Ryder truck used to blow up the Murrah Federal Building in Oklahoma City—and a single container ship can carry as many as 8,000 containers at one time.

Containers could easily be exploited to detonate a bomb that would destroy a bridge, seaport, or other critical infrastructure, causing mass destruction and killing thousands.

Worse, a suitcase-sized nuclear device or radiological "dirty bomb" could also be installed in a container and shipped to the United States. The odds are that the container would never be inspected.

And, even if the container was inspected, it would be too late. The weapon would already be in the United States—most likely near a major population center.

In addition, any attack on or through a seaport could have devastating economic consequences.

Excluding trade with Mexico and Canada, America's ports handle 95 percent of U.S. trade. Every year U.S. ports handle over 800 million tons of cargo valued at approximately \$600 billion.

The West Coast labor disruption last year cost the U.S. economy somewhere \$1–2 billion a day—a total of \$10–20 billion. A terrorist attack would have an ever graver impact.

The U.S. would likely shut down all major U.S. ports, bringing thousands of factories to a standstill and leaving retailers with bare shelves within days. And this shut down will have a ripple effect around the globe, raising the cost exponentially.

In its December 2002 report, the Hart-Rudman Terrorism Task Force discussed the implications of a possible terrorist attack at a seaport. Here is what they said:

If an explosive device were loaded in a container and set off in a port, it would almost automatically raise concern about the integrity of the 21,000 containers that arrive in U.S. ports each day and the many thousands more that arrive by truck and rail across U.S. land borders. A three-to-four-week closure of U.S. ports would bring the global container industry to its knees. Megaports such as Rotterdam and Singapore would have to close their gates to prevent boxes from piling up on their limited pier space. Trucks, trains, and barges would be stranded outside the terminals with no way to unload their boxes. Boxes bound for the United States would have to be unloaded from their outbound ships. Service contracts would need to be renegotiated. As the system became gridlocked, so would much of global commerce.

I am particularly concerned about such an attack because such an enormous proportion of U.S. foreign trade passes through my home state of California.

Last year, 6.2 million imported containers—48 percent—passed through California, 5.7 million just through two ports alone: the Port of Los Angeles and the Port of Long Beach.

That means that, if terrorists succeeded in putting a weapon of mass destruction into a container undetected, there is about a one in two chance that this weapon would arrive and/or be detonated in Southern California.

And the problem is not just with containers.

Nearly one-quarter of all of California's imported crude oil is offloaded in one area. A suicide attack on a tanker at an offloading facility in this area could leave Southern California without refined fuels within a few days.

There is no doubt in my mind that terrorists are seeking to exploit vulnerabilities at our seaports right now.

Indeed, the Al Qaeda training manual specifically mentions seaports as a point of vulnerability in our security.

In addition, we know that Al Qaeda has already tried to attack American interests at and through seaports in the past. Let me mention some examples.

In October 2001, Italian authorities found an Egyptian man suspected of

having ties to Al Qaeda in a container bound for Canada. He had false identifications, maps of airports, a computer, a satellite phone, cameras, and plenty of cash on hand.

In October 2000, Al Qaeda operatives successfully carried out a deadly bombing attack against the U.S.S. *Cole* in the port of Yemen.

In 1998, Al Qaeda bombed the American Embassies in Kenya and Tanzania. Evidence suggests that the explosives the terrorists used were shipped to them by sea. And the investigation of the embassy bombings concluded that Bin Laden has close financial ties to various shipping companies.

We cannot afford to be complacent. Terrorists can be very patient. We cannot forget the successful attack on the World Trade Center on September 11 took place eight years after a relatively unsuccessful attack on the same target.

I introduced legislation in the last Congress to offer a comprehensive solution to the problem of seaport vulnerability. I am pleased that some of its provisions we adopted in some form by recent regulatory changes as well as the Maritime Transportation Security Act of 2002 and Trade Act of 2002.

For example, one provision in my bill required shippers to provide manifest information to Customs at least 24 hours before departure from a foreign port. Soon after the bill was introduced, Customs published a draft regulation with the same requirement.

This requirement is now being enforced. However, Customs is still not getting all relevant information from every important party involved in the shipping process.

In addition, I am pleased that, especially in the last six months, Customs has aggressively promoted its Container Security Initiative (CSI). One of the core elements of this initiative involves placing U.S. Customs inspectors at major foreign seaports to pre-screen cargo containers before they were shipped to America.

Most of the biggest ports in the world are now participating in CSI. However, Customs has posted relatively few inspectors overseas and I believe that CSI can and should be expanded further.

The Maritime Transportation Safety Act of 2002 and Trade Act of 2002 also included a number of security measures.

However, in my view, many of these measures do not go nearly far enough, particularly in the areas of criminal penalties, pushing back the border, minimum port and security standards, employee identification cards, research and development, and so on. And even the strongest provisions in these bills are, in some cases, years away from implementation.

The bottom line is that, while we have made some modest improvements in seaport security in the last year, much more remains to be done. And, crucially, much remains to be done right now.

In fact, I believe that our seaports remain almost as vulnerable today as they were before September 11. That is why I am introducing the Anti-Terrorism and Port Security Act of 2003.

This legislation builds on improvements made to our laws in the last year but goes much further than those changes to ensure the security of our seaports.

The Anti-Terrorism and Port Security Act of 2003 does three main things:

First, the bill ensure that our criminal laws apply to deter and punish terrorists who choose to strike against our seaports. The bill closes a number of loopholes in our criminal laws to ensure that terrorists are held accountable for any attacks. Let me provide a couple of examples.

If a person blows up an airplane, he commits a crime. However, if he blows up an oil tanker, he does not commit a crime—unless he is doing it to injure the person.

If a person distributes explosives to a non-U.S. national, he commits a crime. But if the same person sows mines in the San Francisco harbor, he does not commit a crime.

Specifically, the bill would: Make it a crime for terrorists to attack a port or a cruise ship or deploy a weapon of mass destruction at or through a seaport. Make it a crime to put devices in U.S. waters that can destroy a ship or cargo or interfere with safe navigation or maritime commerce. Update our federal criminal piracy and privateering laws and increase penalties. Make it a crime to use a dangerous weapon or explosive to try to kill someone on board a passenger vessel. Make it a crime to fail to heave to (that is, to slow or stop) a vessel at the direction of a Coast Guard or other authorized federal law enforcement official seeking to board that vessel or to interfere with boarding by such an officer. Make it a crime to destroy an aid to maritime navigation, such as a buoy or shoal/breakwater light, maintained by the Coast Guard if this would endanger the safe navigation of a vessel. Make it a crime for terrorists or criminals to try to attack U.S. citizens or U.S. marine live by putting poisons in the water off shore. Require the Attorney General to issue regulations making it easier to determine the extent of crime and terrorism at seaports and improve communication between different law enforcement agencies involved at ports.

Second, the bill would help improve physical security at seaports by beefing up standards and ensuring greater coordination. Specific provisions would: Designate the Captain-of-the-Port as the primary authority for seaport security at each port. This would enable all parties involved in business at a port to understand who has final say on all security matters. Require minimum federal security standards for ports. These standards include restrictions on private vehicle access, a prohibition on unauthorized

guns and explosives, and unauthorized physical access to terminal areas. They would also mandate that terminal areas at ports have a secure perimeter, monitored or locked access points, sufficient lighting, and so on. Mandate that all Customs inspectors have personal radiation detection pagers. Require all port employees and contractors to have biometric smart identification cards. Require Captains-of-the-Port to keep sensitive information on the port secure and protected. Such information would include, but not be limited to maps, blueprints, and information on the Internet.

Third, the bill would ensure that we devote our limited cargo inspection resources in the most efficient and effective manner. The bill would improve our shipment profiling system by requiring additional information from more relevant parties to the shipping process, and it would substantially improve container security. Specifically, it would establish a comprehensive risk profiling plan for the Customs Service to focus their limited inspection capabilities on high-risk cargo and containers. Under this plan, all relevant parties in the shipment process would provide electronically relevant and timely information to enable Customs to determine which shipments to inspect. Impose steep monetary sanctions for failure to comply with information filing requirements, including filing incorrect information (the current penalty is only up to a few thousand dollars). The Seaport Commission found that about 1/2 of the information on ship manifests was inaccurate. Push U.S. security scrutiny beyond our nation's borders and improve our ability to monitor and inspect cargo and containers before they arrive near America's shores. If a weapon of mass destruction arrives in a U.S. port, it is too late. Require the use of high security seals on all containers coming into the U.S. Require that each container to be transported through U.S. ports receive a universal transaction number that could be used to track container movement from origin to destination. Require all empty containers destined for U.S. ports to be secured. Authorize pilot programs to develop high-tech seals and sensors, including those that would provide real-time evidence of container tampering to a monitor at a terminal. Require ports to provide space to Customs so that the agency is able to use non-intrusive inspection technology. In many cases, Customs has to keep this technology outside the port and bring it in every day, which prevents some of the best inspection technology (which is not portable) from being used. Require the Department of Homeland Security to take the relative number of imported containers received at each port into account in exercising its discretion in determining the allocation of funds appropriated for seaport security grants.

I believe that the Anti-Terrorism and Port Security Act of 2003 would make a

significant contribution to protecting America from terrorist attacks at or through our seaports. I urge my colleagues to support the legislation.;

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

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

S. 746

*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 “Anti-Terrorism and Port Security Act of 2003”.

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

Sec. 1. Short title; table of contents.

**TITLE I—DETECTING AND PUNISHING TERRORISM AND CRIME AT UNITED STATES PORTS**

Sec. 101. Destruction or interference with vessels or maritime facilities.

Sec. 102. Criminal sanctions for placement of destructive devices or substances in United States jurisdictional waters.

Sec. 103. Piracy and privateering.

Sec. 104. Use of a dangerous weapon or explosive on a passenger vessel.

Sec. 105. Sanctions for failure to heave to and for obstruction of boarding and providing false information.

Sec. 106. Criminal sanctions for violence against maritime navigation.

Sec. 107. Criminal sanctions for malicious dumping.

Sec. 108. Attorney general to coordinate port-related crime data collection.

**TITLE II—PROTECTING UNITED STATES PORTS AGAINST TERRORISM AND CRIME**

Subtitle A—General Provision

Sec. 201. Definitions.

Subtitle B—Security Authority

Sec. 211. Designated security authority.

Subtitle C—Securing the Supply Chain

Sec. 221. Manifest requirements.

Sec. 222. Penalties for inaccurate manifest.

Sec. 223. Shipment profiling plan.

Sec. 224. Inspection of merchandise at foreign facilities.

Subtitle D—Security of Seaports and Containers

Sec. 231. Seaport security requirements.

Sec. 232. Seaport security cards.

Sec. 233. Securing sensitive information.

Sec. 234. Container security.

Sec. 235. Office and inspection facilities.

Sec. 236. Security grants to seaports.

**TITLE III—AUTHORIZATION**

Sec. 301. Authorization of appropriations.

**TITLE I—DETECTING AND PUNISHING TERRORISM AND CRIME AT UNITED STATES PORTS**

**SEC. 101. DESTRUCTION OR INTERFERENCE WITH VESSELS OR MARITIME FACILITIES.**

(a) IN GENERAL.—Title 18, United States Code, is amended by inserting after chapter 65 the following:

**“CHAPTER 66—MARITIME VESSELS**

“Sec.

“1371. Jurisdiction and scope.

“1372. Destruction of vessel or maritime facility.

“1373. Imparting or conveying false information.

**“§ 1371 Jurisdiction and scope**

“(a) IN GENERAL.—There is jurisdiction under section 3231 over an offense under this chapter if—

“(1) the prohibited activity takes place within the United States, or in waters or submerged lands thereunder subject to the jurisdiction of the United States; or

“(2) the prohibited activity takes place outside the United States, and—

“(A) an offender or a victim of the prohibited activity is a citizen of the United States;

“(B) a citizen of the United States was on board a vessel to which this chapter applies; or

“(C) the prohibited activity involves a vessel of the United States.

“(b) APPLICABILITY.—Nothing in this chapter shall apply to otherwise lawful activities carried out by, or at the direction of, the United States Government.

**“§ 1372. Destruction of vessel or maritime facility**

“(a) OFFENSES.—It shall be unlawful for any person—

“(1) to willfully—

“(A) set fire to, damage, destroy, disable, or wreck any vessel; or

“(B) place or cause to be placed a destructive device or destructive substance in, upon, or in proximity to, or otherwise make or cause to be made an unworkable or unusable or hazardous to work or use, any vessel (as defined in section 3 of title 1), or any part or other materials used or intended to be used in connection with the operation of a vessel; or

“(C) set fire to, damage, destroy, disable, or displace a destructive device or destructive substance in, upon, or in proximity to, any maritime facility, including any aid to navigation, lock, canal, or vessel traffic service facility or equipment, or interfere by force or violence with the operation of such maritime facility, if such action is likely to endanger the safety of any vessel in navigation;

“(D) set fire to, damage, destroy, disable, or place a destructive device or destructive substance in, upon, or in proximity to any appliance, structure, property, machine, apparatus, or any facility or other material used or intended to be used in connection with the operation, maintenance, loading, unloading, or storage of any vessel or any passenger or cargo carried on, or intended to be carried on, any vessel;

“(E) perform an act of violence against or incapacitate an individual on a vessel, if such act of violence or incapacitation is likely to endanger the safety of the vessel or those on board;

“(F) perform an act of violence against a person that causes or is likely to cause serious bodily injury in, upon, or in proximity to any appliance, structure, property, machine, apparatus, or any facility or other material used or intended to be used in connection with the operation, maintenance, loading, unloading, or storage of any vessel or any passenger or cargo carried or intended to be carried on any vessel; or

“(G) communicate information, knowing the information to be false and under circumstances in which such information may reasonably be believed, thereby endangering the safety of any vessel in navigation; or

“(2) to attempt or conspire to do anything prohibited under paragraph (1).

“(b) PENALTY.—Any person who—

“(1) violates subparagraph (A) or (B) of subsection (a)(1) shall be fined in accordance with this title or imprisoned for a maximum life imprisonment term, or both, and if death results, shall be subject to the death penalty; and

“(2) violates subsection (a)(2) or subparagraph (C), (D), (E), (F), or (G) of subsection (a)(1) shall be fined in accordance with this title or imprisoned not more than 20 years, or both.

“(c) ADDITIONAL PENALTIES.—Any person who is fined or imprisoned in accordance with subsection (b) for an offense that involved a vessel that, at the time the violation occurred, carried high-level radioactive waste or spent nuclear fuel shall be fined in accordance with this title or imprisoned for not less than 30 years, or for life.

“(d) THREATENED OFFENSE.—Any person who willfully imparts or conveys any threat to do an act which would violate this chapter, with an apparent determination and will to carry out the threat, shall be—

“(1) fined in accordance with this title or imprisoned not more than 5 years, or both; and

“(2) liable for all costs incurred as a result of such threat.

“(e) DEFINITIONS.—For purposes of this section—

“(1) the term ‘destructive device’ has the meaning as such term in section 921(a)(4);

“(2) the term ‘destructive substance’ has the meaning as such term in section 31;

“(3) the term ‘high-level radioactive waste’ has the meaning as such term in section 2(12) of the Nuclear Waste Policy Act of 1982 (42 U.S.C. 10101(12));

“(4) the term ‘serious bodily injury’ has the meaning as such term in section 1365(g); and

“(5) the term ‘spent nuclear fuel’ has the meaning as such term in section 2(23) of the Nuclear Waste Policy Act of 1982 (42 U.S.C. 10101(23)).

**“§ 1373. Imparting or conveying false information**

“(a) IN GENERAL.—Any person who imparts or conveys, or causes to be imparted or conveyed, false information, knowing the information to be false, concerning an attempt or alleged attempt being made or to be made, to do any act that is an offense under this chapter or chapters 2, 97, or 111, shall be subject to a civil penalty of not more than \$5,000, which shall be recoverable in a civil action brought in the name of the United States.

“(b) INCREASED PENALTY.—Any person who willfully and maliciously, or with reckless disregard for the safety of human life, imparts or conveys, or causes to be imparted or conveyed, false information, knowing the information to be false, concerning an attempt or alleged attempt being made by or to be made, to do any act that is an offense under this chapter or chapters 2, 97, or 111, shall be fined in accordance with this title or imprisoned not more than 5 years, or both.”.

(b) TECHNICAL AND CONFORMING AMENDMENT.—The table of chapters at the beginning of title 18, is amended by inserting after the item relating to chapter 65 the following:

**“66. Maritime Vessels ..... 1371”.**  
**SEC. 102. CRIMINAL SANCTIONS FOR PLACEMENT OF DESTRUCTIVE DEVICES OR SUBSTANCES IN UNITED STATES JURISDICTIONAL WATERS.**

(a) IN GENERAL.—Chapter 111 of title 18, United States Code, is amended by inserting after section 2280 the following:

**“§ 2280A. Devices or substances in waters of the United States likely to destroy or damage ships**

“(a) IN GENERAL.—Any person who knowingly places or causes to be placed in waters subject to the jurisdiction of the United States, by any means, a device or substance that is likely to destroy or cause damage to a ship or its cargo, or cause interference with the safe navigation of vessels or interference with maritime commerce, such as by

damaging or destroying marine terminals, facilities, and any other maritime structure or entity used in maritime commerce, with the intent of causing such destruction or damage—

“(1) shall be fined in accordance with this title and imprisoned for any term of years or for life; and

“(2) if the death of any person results from conduct prohibited under this section, may be punished by death.

“(b) APPLICABILITY.—Nothing in this section shall be construed to apply to otherwise lawfully authorized and conducted activities of the United States Government.”.

(b) TECHNICAL AND CONFORMING AMENDMENT.—The table of sections for chapter 111 of title 18, United States Code, is amended by inserting after the item relating to section 2280 the following:

“2280A. Devices or substances in waters of the United States likely to destroy or damage ships.”.

#### SEC. 103. PIRACY AND PRIVATEERING.

Chapter 81 of title 18, United States Code, is amended to read as follows:

##### “CHAPTER 81—PIRACY AND PRIVATEERING

“Sec.

“1651. Piracy.

“1652. Crimes against United States persons or property on board a ship or maritime structure.

“1653. Crimes against persons on board a ship or maritime structure within the territorial jurisdiction of the United States.

“1654. Crimes by United States citizens or resident aliens.

“1655. Privateering.

“1656. Theft or conversion of vessel, maritime structure, cargo, or effects.

“1657. Intentional wrecking or plunder of a vessel, maritime structure, cargo, or effects.

“1658. Knowing receipt of an illegally acquired vessel, maritime structure, cargo, or effects.

“1659. Attempts.

“1660. Accessories.

“1661. Inapplicability to United States Government activities.

#### “§ 1651. Piracy

“Any person who commits the crime of piracy and is afterwards brought into, or found in, the United States shall be imprisoned for life.

#### “§ 1652. Crimes against United States persons or property on board a ship or maritime structure

“Any person who commits any illegal act of violence, detention, or depredation against the United States, including any vessel of the United States, citizen of the United States, any commercial structure owned in whole or in part by a United States citizen or resident alien, or any United States citizen or resident alien, or the property of that citizen or resident alien, on board a ship or maritime structure and is afterwards brought into or found in the United States, shall be fined in accordance with this title or imprisoned not more than 20 years, or both.

#### “§ 1653. Crimes against persons on board a ship or maritime structure within the territorial jurisdiction of the United States

“Any person who commits any illegal act of violence, detention, or depredation against an individual on board a ship or maritime structure, or the property of that individual, in waters or submerged lands thereunder, subject to the jurisdiction of the United States, shall be fined in accordance

with this title or imprisoned not more than 20 years, or both.

#### “§ 1654. Crimes by United States citizens or resident aliens

“Any person, being a United States citizen or resident alien, or purporting to act under the authority of the United States, who commits any illegal act of violence, detention, or depredation against an individual on board a ship or maritime structure, or the property of that individual, shall be fined in accordance with this title or imprisoned not more than 20 years, or both.

#### “§ 1655. Privateering

“(a) OFFENSE.—It shall be unlawful for any person to furnish, fit out, arm, or serve in a privateer or private vessel used to commit any illegal act of violence, detention, or depredation against an individual, or the property of that individual, or any vessel or maritime structure without the express authority of the United States Government when—

“(1) the perpetrator of the act is a United States citizen or resident alien, or purports to act under authority of the United States;

“(2) the individual against whom the act is committed is a United States citizen or resident alien or the property, vessel, or maritime structure involved is owned, in whole or in part, by a United States citizen or resident alien; or

“(3) some element of the illegal act of violence, detention, or depredation is committed in waters subject to the jurisdiction of the United States.

“(b) PENALTY.—Any person who violates subsection (a) shall be fined in accordance with this title or imprisoned not more than 20 years, or both.

#### “§ 1656. Theft or conversion of vessel, maritime structure, cargo, or effects

“(a) OFFENSE.—It shall be unlawful for any person who is a captain, officer, crewman, or passenger of a vessel or maritime structure to assist in the theft or conversion of such vessel or maritime structure, or its cargo or effects when—

“(1) the perpetrator is a United States citizen or resident alien, or purports to act under the authority of the United States;

“(2) the vessel, maritime structure, cargo, or effects is owned in whole or in part by a United States citizen or resident alien; or

“(3) some element of the theft or conversion is committed in waters subject to the jurisdiction of the United States.

“(b) PENALTY.—Any person who violates subsection (a) shall be fined in accordance with this title or imprisoned not more than 20 years, or both.

#### “§ 1657. Intentional wrecking or plunder of a vessel, maritime structure, cargo, or effects

“(a) OFFENSE.—It shall be unlawful for any person to—

“(1) intentionally cause the wrecking of a vessel or maritime structure by act or omission, either directly such as by intentional grounding, or indirectly by modification or destruction of any navigational marker or safety device;

“(2) intentionally plunder, steal, or destroy a vessel, maritime structure, cargo, or effects when such vessel or maritime structure is in distress, wrecked, lost, stranded, or cast away; or

“(3) intentionally obstruct or interfere with the rescue of a person on board a vessel or maritime structure in distress, wrecked, lost, stranded, or cast away, or the legal salvage of such a vessel, maritime structure, cargo, or effects, when—

“(A) the perpetrator is a United States citizen or resident alien, or purports to act under authority of the United States;

“(B) the vessel, maritime structure, cargo, or effects is owned in whole or in part by a United States citizen or resident alien; or

“(C) some element of the theft or conversion is committed in waters subject to the jurisdiction of the United States.

“(b) PENALTY.—Any person who violates subsection (a) shall be fined in accordance with this title or imprisoned not more than 20 years, or both.

#### “§ 1658. Knowing receipt of an illegally acquired vessel, maritime structure, cargo, or effects

“Any person who knowingly receives or acquires a vessel, maritime structure, cargo, or effects converted or obtained by action falling under any section of this chapter shall be fined in accordance with this title or imprisoned not more than 20 years, or both.

#### “§ 1659. Attempts

Any person who attempts any act which, if committed, would constitute an offense under this chapter shall be fined in accordance with this title or imprisoned not more than 20 years, or both.

#### “§ 1660. Accessories

“(a) COMMISSION OF AN OFFENSE.—Any person who knowingly assists any person in the commission of an act that constitutes an offense under this chapter shall be fined in accordance with this title or imprisoned not more than 20 years, or both.

“(b) AVOIDANCE OF CONSEQUENCES.—Any person who knowingly assists any person in avoiding the consequences of an act that constitutes an offense under this chapter shall be fined in accordance with this title or imprisoned not more than 20 years, or both.

#### “§ 1661. Inapplicability to United States Government activities

“Nothing in this chapter shall apply to otherwise lawful activities—

“(1) carried out by, or at the direction of, the United States Government; or

“(2) undertaken under a letter or marque and reprisal issued by the United States Government.”.

#### SEC. 104. USE OF A DANGEROUS WEAPON OR EXPLOSIVE ON A PASSENGER VESSEL.

(a) IN GENERAL.—Chapter 39 of title 18, United States Code, is amended by inserting after section 831 the following:

##### “§ 832. Use of a dangerous weapon or explosive on a passenger vessel

“(a) OFFENSE.—It shall be unlawful for any person to willfully—

“(1) commit an act, including the use of a dangerous weapon, explosive, or incendiary device, with the intent to cause death or serious bodily injury to a crew member or passenger of a passenger vessel or any other person while on board a passenger vessel; or

“(2) attempt, threaten, or conspire to do any act referred to in paragraph (1).

“(b) PENALTY.—An person who violates subsection (a) shall be fined in accordance with this title or imprisoned not more than 20 years, or both.

“(c) AGGRAVATED OFFENSE.—Any person who commits an offense described in subsection (a) in a circumstance in which—

“(1) the vessel was carrying a passenger at the time of the offense; or

“(2) the offense has resulted in the death of any person;

shall be guilty of an aggravated offense and shall be fined in accordance with this title or imprisoned for any term of years or for life.

“(d) APPLICABILITY.—This section shall apply to vessels that are subject to the jurisdiction of the United States, and vessels carrying passengers who are United States citizens or resident aliens, wherever located.

“(e) DEFINITIONS.—For purposes of this section—

“(1) the term ‘dangerous weapon’ has the meaning given such term in section 930(g);

“(2) the term ‘explosive or incendiary device’ has the meaning given such term in section 232(5);

“(3) the term ‘passenger’ has the same meaning given such term in section 2101(21) of title 46;

“(4) the term ‘passenger vessel’ has the same meaning given such term in section 2101(22) of title 46; and

“(5) the term ‘serious bodily injury’ has the meaning given such term in section 1365(g).”.

(b) TECHNICAL AND CONFORMING AMENDMENT.—The table of sections for chapter 39 of title 18, United States Code, is amended by inserting after the item relating to section 831 the following:

“832. Use of a dangerous weapon or explosive on a passenger vessel.”.

**SEC. 105. SANCTIONS FOR FAILURE TO HEAVE TO AND FOR OBSTRUCTION OF BOARDING AND PROVIDING FALSE INFORMATION.**

(a) IN GENERAL.—Chapter 109 of title 18, United States Code, is amended by adding at the end the following:

**“§2237. Sanctions for failure to heave to; sanctions for obstruction of boarding or providing false information**

“(a) FAILURE TO HEAVE TO.—It shall be unlawful for the master, operator, or person in charge of a vessel of the United States, or a vessel subject to the jurisdiction of the United States, to knowingly fail to obey an order to heave to on being ordered to do so by an authorized Federal law enforcement officer.

“(b) OBSTRUCTION OF BOARDING AND PROVIDING FALSE INFORMATION.—It shall be unlawful for any person on board a vessel of the United States or a vessel subject to the jurisdiction of the United States to—

“(1) forcibly assault, resist, oppose, prevent, impede, intimidate, or interfere with a boarding or other law enforcement action authorized by any Federal law, or to resist a lawful arrest; or

“(2) provide information to a Federal law enforcement officer during a boarding of a vessel regarding the vessel’s destination, origin, ownership, registration, nationality, cargo, or crew that the person knows is false.

“(c) LIMITATIONS.—This section shall not limit the authority of—

“(1) an officer under section 581 of the Tariff Act of 1930 (19 U.S.C. 1581) or any other provision of law enforced or administered by the Secretary of the Treasury or the Under Secretary for Border and Transportation Security of the Department of Homeland Security; or

“(2) a Federal law enforcement officer under any law of the United States to order a vessel to stop or heave to.

“(d) CONSENT OR OBJECTION TO ENFORCEMENT.—A foreign nation may consent or waive objection to the enforcement of United States law by the United States under this section by radio, telephone, or similar oral or electronic means, which consent or waiver may be proven by certification of the Secretary of State or the Secretary’s designee.

“(e) PENALTY.—Any person who intentionally violates this section shall be fined in accordance with this title and imprisoned not more than 1 year.

“(f) DEFINITIONS.—For purposes of this section—

“(1) the terms ‘vessel of the United States’ and ‘vessel subject to the jurisdiction of the United States’ have the same meanings as such terms in section 3 of the Maritime Drug Law Enforcement Act (46 U.S.C. App. 1903);

“(2) the term ‘heave to’ means to cause a vessel to slow, come to a stop, or adjust its course or speed to account for the weather conditions and sea state to facilitate a law enforcement boarding; and

“(3) the term ‘Federal law enforcement officer’ has the same meaning as such term in section 115.”.

(b) TECHNICAL AND CONFORMING AMENDMENT.—The table of sections for chapter 109 of title 18, United States Code, is amended by adding at the end the following:

“2237. Sanctions for failure to heave to; sanctions for obstruction of boarding or providing false information.”.

**SEC. 106. CRIMINAL SANCTIONS FOR VIOLENCE AGAINST MARITIME NAVIGATION.**

Section 2280(a) of title 18, United States Code, is amended—

(1) in paragraph (1)—

(A) by redesignating subparagraphs (F), (G), and (H) as (G), (H), and (I), respectively;

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

“(F) destroys, damages, alters, moves, or tampers with any aid to maritime navigation maintained by the Saint Lawrence Seaway Development Corporation under the authority of section 4 of the Act of May 13, 1954, (33 U.S.C. 984) or the Coast Guard pursuant to section 81 of title 14, or lawfully maintained by the Coast Guard pursuant to section 83 of title 14, if such act endangers or is likely to endanger the safe navigation of a ship;”;

(C) in subparagraph (I), as so redesignated, by striking “through (G)” and inserting “through (H)”;

(2) in paragraph (2), by striking “(C) or (E)” and inserting “(C), (E), or (F)”.

**SEC. 107. CRIMINAL SANCTIONS FOR MALICIOUS DUMPING.**

(a) IN GENERAL.—Chapter 111 of title 18, United States Code, is amended by adding at the end the following:

**“§2282. Knowing discharge or release**

“(a) ENDANGERMENT OF HUMAN LIFE.—Any person who knowingly discharges or releases oil, a hazardous material, a noxious liquid substance, or any other substance into the navigable waters of the United States or the adjoining shoreline with the intent to endanger human life, health, or welfare—

“(1) shall be fined in accordance with this title and imprisoned for any term of years or for life; and

“(2) if the death of any person results from conduct prohibited under this section, may be punished by death.

“(b) ENDANGERMENT OF MARINE ENVIRONMENT.—Any person who knowingly discharges or releases oil, a hazardous material, a noxious liquid substance, or any other substance into the navigable waters of the United States or the adjacent shoreline with the intent to endanger the marine environment shall be fined in accordance with this title or imprisoned not more than 30 years, or both.

“(c) DEFINITIONS.—For purposes of this section—

“(1) the term ‘discharge’ means any spilling, leaking, pumping, pouring, emitting, emptying, or dumping;

“(2) the term ‘hazardous material’ has the same meaning given such term in section 2101(14) of title 46;

“(3) the term ‘marine environment’ has the same meaning given such term in section 2101(15) of title 46;

“(4) the term ‘navigable waters’ has the same meaning given such term in section 502(7) of the Federal Water Pollution Control Act (33 U.S.C. 1362(7)), and also includes the territorial sea of the United States as described in Presidential Proclamation 5928 of December 27, 1988; and

“(5) the term ‘noxious liquid substance’ has the same meaning given such term in the MARPOL Protocol as defined in section 2(a)(3) of the Act to Prevent Pollution from Ships (33 U.S.C. 1901(a)(3)).”.

(b) TECHNICAL AND CONFORMING AMENDMENT.—The table of sections for chapter 111

of title 18, United States Code, is amended by adding at the end the following:

“2282. Knowing discharge or release.”.

**SEC. 108. ATTORNEY GENERAL TO COORDINATE PORT-RELATED CRIME DATA COLLECTION.**

(a) REGULATIONS.—The Attorney General shall issue regulations to—

(1) require the reporting by a carrier that is the victim of a cargo theft offense to the Attorney General of information on the cargo theft offense (including offenses occurring outside ports of entry and ports of shipment origination) that identifies the port of entry, the port where the shipment originated, where the theft occurred, and any other information specified by the Attorney General;

(2) create a database to contain the reports described in paragraph (1) and integrate those reports, to the extent feasible, with other noncriminal justice and intelligence data, such as insurer bill of lading, cargo contents and value, point of origin, and lien holder filings; and

(3) prescribe procedures for access to the database created in accordance with paragraph (2) by appropriate Federal, State, and local governmental agencies and private companies or organizations, while limiting access to privacy of the information in accordance with other applicable Federal laws.

(b) MODIFICATION OF DATABASES.—

(1) IN GENERAL.—United States Government agencies with significant regulatory or law enforcement responsibilities at United States ports shall, to the extent feasible, modify their information databases to ensure the collection and retrievability of data relating to crime, terrorism, and related activities at, or affecting, United States ports.

(2) DESIGNATION OF AGENCIES.—The Attorney General, after consultation with the Secretary of Homeland Security, shall designate the agencies referred to in paragraph (1).

(c) OUTREACH PROGRAM.—The Attorney General, in consultation with the Secretary of Homeland Security, the National Maritime Security Advisory Committee established under section 70112 of title 46, United States Code, and the appropriate Federal and State agencies, shall establish an outreach program—

(1) to work with State and local law enforcement officials to harmonize the reporting of data on cargo theft among States and localities with the United States Government’s reports; and

(2) to work with local port security committees to disseminate cargo theft information to appropriate law enforcement officials.

(d) ANNUAL REPORT.—The Attorney General shall report annually to the Committee on the Judiciary of the Senate and the House of Representatives on the implementation of this section.

(e) INTERSTATE OR FOREIGN SHIPMENTS BY CARRIER; STATE PROSECUTIONS.—

(1) STATE PROSECUTIONS.—Section 659 of title 18, United States Code, is amended—

(A) in the first undesignated paragraph—

(i) by striking “Whoever embezzles” and inserting the following:

“(a) OFFENSE; PENALTY.—Whoever—

“(1) embezzles”;

(ii) by striking “from any pipeline system” and all that follows through “with intent to convert to his own use”;

(iii) by striking “or” at the end;

(B) in the second undesignated paragraph—

(i) by striking “Whoever buys” and inserting the following:

“(2) buys”;

(ii) by striking “or” at the end;

(C) in the third undesignated paragraph—

(i) by striking “Whoever embezzles” and inserting the following”

“(3) embezzles”; and

(ii) by striking “with intent to convert to his own use”;

(D) in the fourth undesignated paragraph, by striking “Whoever embezzles” and inserting the following:

“(4) embezzles”;

(E) in the fifth undesignated paragraph, by striking “Shall in each case” and inserting the following:

“shall in each case”;

(F) in the sixth undesignated paragraph, by striking “The” and inserting the following:

“(b) LOCATION OF OFFENSE.—The”;

(G) in the seventh undesignated paragraph, by striking “The” and inserting the following:

“(c) SEPARATE OFFENSE.—The”;

(H) in the eighth undesignated paragraph, by striking “To” and inserting the following:

“(d) PRIMA FACIE EVIDENCE.—To”;

(I) in the ninth undesignated paragraph, by striking “A” and inserting the following:

“(e) PROSECUTION.—A”;

(J) by adding at the end the following:

“(f) CIVIL PENALTY.—

“(1) IN GENERAL.—Notwithstanding any other provision of law, and in addition to any penalties that may be available under any other provision of law, a person who is found by the Secretary of Homeland Security, after notice and an opportunity for a hearing, to have violated this section or a regulation issued under this section shall be liable to the United States for a civil penalty not to exceed \$25,000 for each violation.

“(2) SEPARATE VIOLATIONS.—Each day of a continuing violation shall constitute a separate violation.

“(3) AMOUNT OF PENALTY.—

“(A) IN GENERAL.—The amount of a civil penalty for a violation of this section or a regulation issued under this section shall be assessed by the Attorney General, or the designee of the Attorney General, by written notice.

“(B) CONSIDERATIONS.—In determining the amount of a civil penalty under this paragraph, the Attorney General shall take into account—

“(i) the nature, circumstances, extent, and gravity of the prohibited act committed; and

“(ii) with respect to the violator, the degree of culpability, any history of prior offenses, ability to pay, and such other matters as justice may require.

“(4) MODIFICATION OF PENALTY.—The Secretary of Homeland Security may compromise, modify, or remit, with or without conditions, any civil penalty that is subject to imposition or which has been imposed under this section.

“(5) FAILURE TO PAY.—If a person fails to pay an assessment of a civil penalty after it has become final, the Secretary of Homeland Security may refer the matter to the Attorney General for collection in an appropriate district court of the United States.

“(g) DEFINITION.—For purposes of this section, the term ‘goods or chattels’ means to be moving as an interstate or foreign shipment at all points between the point of origin and the final destination (as evidenced by the waybill or other shipping document of the shipment) regardless of any temporary stop while awaiting transshipment or otherwise.”

(2) FEDERAL SENTENCING GUIDELINES.—Pursuant to section 994 of title 28, United States Code, the United States Sentencing Commission shall review the Federal Sentencing Guidelines to determine whether sentencing enhancement is appropriate for any offense under section 659 of title 18, United States Code, as amended by this subsection.

(3) ANNUAL REPORT.—The Attorney General shall annually submit to Congress a report

that shall include an evaluation of law enforcement activities relating to the investigation and prosecution of offenses under section 659 of title 18, United States Code.

**TITLE II—PROTECTING UNITED STATES PORTS AGAINST TERRORISM AND CRIME**

**Subtitle A—General Provision**

**SEC. 201. DEFINITIONS.**

In this title:

(1) AIRCRAFT.—The term “aircraft” has the meaning given that term in section 40102 of title 49, United States Code.

(2) CAPTAIN-OF-THE-PORT.—The term “Captain-of-the-Port”, with respect to a United States seaport, means the individual designated by the Commandant of the Coast Guard as the Captain-of-the-Port at that seaport.

(3) COMMON CARRIER.—The term “common carrier” means any person that holds itself out to the general public as a provider for hire of a transportation by water, land, or air of merchandise, whether or not the person actually operates the vessel, vehicle, or aircraft by which the transportation is provided, between a port or place and a port or place in the United States.

(4) CONTAINER.—The term “container” means a container that is used or designed for use for the international transportation of merchandise by vessel, vehicle, or aircraft.

(5) DIRECTORATE.—The term “Directorate” means the Border and Transportation Security Directorate of the Department of Homeland Security.

(6) MANUFACTURER.—The term “manufacturer” means a person who fabricates or assembles merchandise for sale in commerce.

(7) MERCHANDISE.—The term “merchandise” has the meaning given that term in section 401 of the Tariff Act of 1930 (19 U.S.C. 1401).

(8) OCEAN TRANSPORTATION INTERMEDIARY.—The term “ocean transportation intermediary” has the meaning given that term in section 515.2 of title 46, Code of Federal Regulations (as in effect on January 1, 2003).

(9) SHIPMENT.—The term “shipment” means cargo traveling in international commerce under a bill of lading.

(10) SHIPPER.—The term “shipper” means—

(A) a cargo owner;

(B) the person for whose account ocean transportation is provided;

(C) the person to whom delivery of merchandise is to be made; or

(D) a common carrier that accepts responsibility for payment of all charges applicable under a tariff or service contract.

(11) UNITED STATES SEAPORT.—The term “United States seaport” means a place in the United States on a waterway with shore-side facilities for the intermodal transfer of cargo containers that are used in international trade.

(12) VEHICLE.—The term “vehicle” has the meaning given that term in section 401 of the Tariff Act of 1930 (19 U.S.C. 1401).

(13) VESSEL.—The term “vessel” has the meaning given that term in section 401 of the Tariff Act of 1930 (19 U.S.C. 1401).

**Subtitle B—Security Authority**

**SEC. 211. DESIGNATED SECURITY AUTHORITY.**

The Captain-of-the-Port of each United States seaport shall be the primary authority responsible for security at the United States seaport and shall—

(1) coordinate security at such seaport; and

(2) be the point of contact on seaport security issues for civilian and commercial port entities at such seaport.

**Subtitle C—Securing the Supply Chain**

**SEC. 221. MANIFEST REQUIREMENTS.**

Section 431(b) of the Tariff Act of 1930 (19 U.S.C. 1431(b)) is amended—

(1) by striking “Any manifest” and inserting the following:

“(1) IN GENERAL.—Any manifest”; and

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

“(2) REQUIRED INFORMATION.—

“(A) REQUIREMENT.—In addition to any other requirement under this section, the pilot, master, operator, or owner (or the authorized agent of such operator or owner) of every vessel required to make entry or obtain clearance under the laws of the United States shall transmit electronically the cargo manifest information described in subparagraph (B) in such manner and form as the Secretary shall prescribe. The Secretary shall ensure the electronic information is maintained securely, and is available only to individuals with Federal Government security responsibilities.

“(B) CONTENT.—The cargo manifest required by subparagraph (A) shall consist of the following information:

“(i) The port of arrival and departure.

“(ii) The carrier code assigned to the shipment.

“(iii) The flight, voyage, or trip number.

“(iv) The dates of scheduled arrival and departure.

“(v) A request for a permit to proceed to the destination, if such permit is required.

“(vi) The numbers and quantities from the carrier’s master airway bill, bills of lading, or ocean bills of lading.

“(vii) The first port of lading of the cargo and the city in which the carrier took receipt of the cargo.

“(viii) A description and weight of the cargo (including the Harmonized Tariff Schedule of the United States number under which the cargo is classified) or, for a sealed container, the shipper’s declared description and weight of the cargo.

“(ix) The shipper’s name and address, or an identification number, from all airway bills and bills of lading.

“(x) The consignee’s name and address, or an identification number, from all airway bills and bills of lading.

“(xi) Notice of any discrepancy between actual boarded quantities and airway bill or bill of lading quantities, except that a carrier is not required by this clause to verify boarded quantities of cargo in sealed containers.

“(xii) Transfer or transit information for the cargo while it has been under the control of the carrier.

“(xiii) The location of the warehouse or other facility where the cargo was stored while under the control of the carrier.

“(xiv) The name and address, or identification number of the carrier’s customer including the forwarder, nonvessel operating common carrier, and consolidator.

“(xv) The conveyance name, national flag, and tail number, vessel number, or train number.

“(xvi) The country of origin and ultimate destination.

“(xvii) The carrier’s reference number, including the booking or bill number.

“(xviii) The shipper’s commercial invoice number and purchase order number.

“(xix) Information regarding any hazardous material contained in the cargo.

“(xx) License information including the license code, license number, or exemption code.

“(xxi) The container number for containerized shipments.

“(xxii) Certification of the empty condition of any empty containers.

“(xxiii) Any additional information that the Secretary, in consultation with the Secretary of Homeland Security, by regulation determines is reasonably necessary to ensure

aviation, maritime, and surface transportation safety pursuant to the laws enforced and administered by the Secretary or the Under Secretary for Border and Transportation Security of the Department of Homeland Security.”.

**SEC. 222. PENALTIES FOR INACCURATE MANIFEST.**

(a) FALSITY OR LACK OF MANIFEST.—Section 584 of the Tariff Act of 1930 (19 U.S.C. 1584) is amended—

(1) in subsection (a)(1)—

(A) by striking “\$1,000” each place it appears and inserting “\$50,000”; and

(B) by striking “\$10,000” and inserting “\$50,000”; and

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

“(c) CRIMINAL PENALTIES.—Any person who ships or prepares for shipment any merchandise bound for the United States who intentionally provides inaccurate or false information, whether inside or outside the United States, with respect to such merchandise for the purpose of introducing such merchandise into the United States in violation of the laws of the United States, shall be liable, upon conviction of a violation of this subsection, for a fine of not more than \$50,000 or imprisonment for 1 year, or both; except that if the importation of such merchandise into the United States is prohibited, such person shall be liable for an additional fine of not more than \$50,000 or imprisonment for not more than 5 years, or both.”.

(b) PENALTIES FOR VIOLATIONS OF THE ARRIVAL, REPORTING, ENTRY, AND CLEARANCE REQUIREMENTS.—Subsections (b) and (c) of section 436 of Tariff Act of 1930 (19 U.S.C. 1436) are amended to read as follows:

“(b) CIVIL PENALTY.—Any master, person in charge of a vessel, vehicle, or aircraft pilot who commits any violation listed in subsection (a) shall be liable for a civil penalty of \$25,000 for the first violation, and \$50,000 for each subsequent violation, and any conveyance used in connection with any such violation is subject to seizure and forfeiture.

“(c) CRIMINAL PENALTY.—In addition to being liable for a civil penalty under subsection (b), any master, person in charge of a vessel, vehicle, or aircraft pilot who intentionally commits or causes another to commit any violation listed in subsection (a) shall be liable, upon conviction, for a fine of not more than \$50,000 or imprisonment for 1 year, or both; except that if the conveyance has, or is discovered to have had, on board any merchandise (other than sea stores or the equivalent for conveyances other than vessels) the importation of which into the United States is prohibited, such individual shall be liable for an additional fine of not more than \$50,000 or imprisonment for not more than 5 years, or both.”.

**SEC. 223. SHIPMENT PROFILING PLAN.**

(a) IN GENERAL.—The Secretary of Homeland Security shall develop a shipment profiling plan to track containers and shipments of merchandise to be imported into the United States. The tracking system shall be designed to identify any shipment that is a threat to the security of the United States before such shipment enters the United States.

(b) INFORMATION REQUIREMENTS.—

(1) CONTENT.—The shipment profiling plan required by subsection (a) shall at a minimum—

(A) require common carriers, shippers, and ocean transportation intermediaries to provide appropriate information regarding each shipment of merchandise, including the information required under section 431(b) of the Tariff Act of 1930 (19 U.S.C. 1431(b)) to the Secretary of Homeland Security; and

(B) require shippers to use a standard international bill of lading for each shipment that includes—

(i) the weight of the cargo;  
(ii) the value of the cargo;  
(iii) the vessel name;  
(iv) the voyage number;  
(v) a description of each container;  
(vi) a description of the nature, type, and contents of the shipment;  
(vii) the code number from the Harmonized

Tariff Schedule;

(viii) the port of destination;  
(ix) the final destination of the cargo;  
(x) the means of conveyance of the cargo;  
(xi) the origin of the cargo;  
(xii) the name of the precarriage deliverer or agent;  
(xiii) the port at which the cargo was load-

ed;

(xiv) the name of the formatting agent;

(xv) the bill of lading number;

(xvi) the name of the shipper;

(xvii) the name of the consignee;

(xviii) the universal transaction number or carrier code assigned to the shipper by the Secretary;

(xix) the information contained in the continuous synopsis record for the vessel transporting the shipment; and

(xx) any additional information that the Secretary by regulation determines is reasonably necessary to ensure seaport safety.

(2) CONTINUOUS SYNOPSIS RECORD DEFINED.—

In this subsection, the term “continuous synopsis record” means the continuous synopsis record required by regulation 5 of chapter XI-1 of the Annex to the International Convention of the Safety of Life at Sea, 1974.

(3) EFFECTIVE DATE.—The requirement imposed under clause (xix) of paragraph (1)(B) shall take effect on July 1, 2004.

(c) CREATION OF PROFILE.—The Secretary of Homeland Security shall combine the information described in subsection (b) with other law enforcement and national security information that the Secretary determines useful to assist in locating containers and shipments that could pose a threat to the security of the United States and to create a profile of every container and every shipment within the container that will enter the United States.

(d) CARGO SCREENING.—

(1) IN GENERAL.—Officers of the Directorate shall review the profile of a shipment that a shipper desires to transport into the United States to determine whether the shipment or the container in which it is carried should be subjected to additional inspection by the Directorate. In making such a determination, an officer shall consider, in addition to any other relevant factors—

(A) whether the shipper has regularly shipped cargo to the United States in the past; and

(B) the specificity of the description of the shipment’s contents.

(2) NOTIFICATION.—The Secretary of Homeland Security shall transmit to the shipper and the person in charge of the vessel, aircraft, or vehicle on which a shipment is located a notification of whether the shipment is to be subjected to additional inspection as described in paragraph (1).

(e) CONSISTENCY WITH THE NATIONAL CUSTOMS AUTOMATION PROGRAM.—The Secretary of Homeland Security, in consultation with the Secretary of the Treasury, shall ensure that the National Customs Automation Program established pursuant to section 411 of the Tariff Act of 1930 (19 U.S.C. 1411) is compatible with the shipment profile plan developed under this section.

**SEC. 224. INSPECTION OF MERCHANDISE AT FOREIGN FACILITIES.**

Not later than 180 days after the date of enactment of this Act, the Secretary of

Homeland Security shall submit to Congress a plan to—

(1) station inspectors from the Directorate, other Federal agencies, or the private sector at the foreign facilities of manufacturers or common carriers to profile and inspect merchandise and the containers or other means by which such merchandise is transported as they are prepared for shipment on a vessel that will arrive at any port or place in the United States;

(2) develop procedures to ensure the security of merchandise inspected as described in paragraph (1) until it reaches the United States; and

(3) permit merchandise inspected as described in paragraph (1) to receive expedited inspection upon arrival in the United States.

**Subtitle D—Security of Seaports and Containers**

**SEC. 231. SEAPORT SECURITY REQUIREMENTS.**

(a) REQUIREMENT.—Not later than 180 days after the date of enactment of this Act, the Secretary of Homeland Security shall issue final regulations setting forth minimum security requirements, including security performance standards for United States seaports. The regulations shall—

(1) limit private vehicle access to the terminal area of a United States seaport to vehicles that are registered at such seaport and display a seaport registration pass;

(2) prohibit individuals, other than law enforcement officers, from carrying firearms or explosives inside a United States seaport without written authorization from the Captain-of-the-Port;

(3) prohibit individuals from physically accessing the terminal area of a United States seaport without a seaport specific access pass;

(4) require that officers of the Directorate, and other appropriate law enforcement officers, at United States seaports be provided with, and utilize, personal radiation detection pagers to increase the ability of such officers to accurately detect radioactive materials that could be used to commit terrorist acts in the United States;

(5) require that the terminal area of each United States seaport be equipped with—

(A) a secure perimeter;

(B) monitored or locked access points; and

(C) sufficient lighting; and

(6) include any additional security requirement that the Secretary determines is reasonably necessary to ensure seaport security.

(b) LIMITATION.—Except as provided in subsection (c), any United States seaport that does not meet the minimum security requirements described in subsection (a) is prohibited from—

(1) handling, storing, stowing, loading, discharging, or transporting dangerous cargo; and

(2) transferring passengers to or from a passenger vessel that—

(A) weighs more than 100 gross tons;

(B) carries more than 12 passengers for hire; and

(C) has a planned voyage of more than 24 hours, part of which is on the high seas.

(c) EXCEPTION.—The Secretary of Homeland Security may waive 1 or more of the minimum requirements described in subsection (a) for a United States seaport if the Secretary determines that it is not appropriate for such seaport to implement the requirement.

**SEC. 232. SEAPORT SECURITY CARDS.**

Section 70105 of title 46, United States Code, is amended—

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

“(a) PROHIBITION.—(1) Unless the requirements of paragraph (2) are met, the Secretary shall prescribe regulations to prohibit—

“(A) an individual from entering an area of a vessel or facility that is designated as a secure area by the Secretary for purposes of a security plan for the vessel or facility that is approved by the Secretary under section 70103 of this title; and

“(B) an individual who is regularly employed at a United States seaport or who is employed by a common carrier that transports merchandise to or from a United States seaport from entering a United States seaport.

“(2) The prohibition imposed under paragraph (1) may not apply to—

“(A) an individual who—

“(i) holds a transportation security card issued under this section; and

“(ii) is authorized to be in area in accordance with the plan if the individual is attempting to enter an area of a vessel or facility that is designated as a secure area by the Secretary for purposes of a security plan for the vessel or facility approved by the Secretary under section 70103 of this title; or

“(B) an individual who is accompanied by another individual who may access the secure area or United States seaport in accordance with this section.

“(3) A person may not admit an individual into a United States seaport or a secure area unless the individual is in compliance with this subsection.”;

(2) in paragraph (2) of subsection (b)—

(A) in subparagraph (E), by striking “and”;

(B) by redesignating subparagraph (F) as subparagraph (G); and

(C) by inserting after subparagraph (E) the following new subparagraph:

“(F) an individual who is regularly employed at a United States seaport or who is employed by a common carrier that transports merchandise to or from a United States seaport; and”;

(3) in paragraph (1) of subsection (c)—

(A) in subparagraph (C), by striking “or”;

(B) in subparagraph (D), by striking the period at the end and inserting a semicolon and “or”;

(C) at the end, by inserting the following new subparagraph:

“(E) has not provided sufficient information to allow the Secretary to make the determinations described in subparagraph (A), (B), (C), or (D).”;

(4) by striking subsection (f); and

(5) by inserting after subsection (e) the following new subsections:

“(f) DATA ON CARDS.—A transportation security card issued under this section shall—

“(1) be tamper resistant; and

“(2) contain—

“(A) the number of the individual’s commercial driver’s license issued under chapter 313 of title 49, if any;

“(B) the State-issued vehicle registration number of any vehicle that the individual desires to bring into the United States seaport, if any;

“(C) the work permit number issued to the individual, if any;

“(D) a unique biometric identifier to identify the license holder; and

“(E) a safety rating assigned to the individual by the Secretary of Homeland Security.

“(g) DEFINITIONS.—In this section:

“(1) ALIEN.—The term ‘alien’ has the meaning given the term in section 101(a)(3) of the Immigration and Nationality Act (8 U.S.C. 1101(a)(3)).

“(2) UNITED STATES SEAPORT.—The term ‘United States seaport’ means a place in the United States on a waterway with shoreside facilities for the intermodal transfer of cargo

containers that are used in international trade.”.

#### SEC. 233. SECURING SENSITIVE INFORMATION.

(a) REQUIREMENT.—Not later than 90 days after the date of enactment of this Act, the Captain-of-the-Port of each United States seaport shall secure and protect all sensitive information, including information that is currently available to the public, related to the seaport.

(b) SENSITIVE INFORMATION.—In this section, the term “sensitive information” means—

(1) maps of the seaport;

(2) blueprints of structures located within the seaport; and

(3) any other information related to the security of the seaport that the Captain-of-the-Port determines is appropriate to secure and protect.

#### SEC. 234. CONTAINER SECURITY.

(a) CONTAINER SEALS.—

(1) APPROVAL.—Not later than 90 days after the date of enactment of this Act, the Secretary of Homeland Security shall approve minimum standards for high security container seals that—

(A) meet or exceed the American Society for Testing Materials Level D seals;

(B) permit each seal to have a unique identification number; and

(C) contain an electronic tag that can be read electronically at a seaport.

(2) REQUIREMENT FOR USE.—Within 180 days after the date of enactment of this Act, the Secretary of Homeland Security shall deny entry of a vessel into the United States if the containers carried by the vessel are not sealed with a high security container seal approved under paragraph (1).

(b) IDENTIFICATION NUMBER.—

(1) REQUIREMENT.—A shipment that is shipped to or from the United States either directly or via a foreign port shall have a designated universal transaction number.

(2) TRACKING.—The person responsible for the security of a container shall record the universal transaction number assigned to the shipment under paragraph (1), as well as any seal identification number on the container, at every port of entry and point at which the container is transferred from one conveyance to another conveyance.

(c) PILOT PROGRAM.—

(1) GRANTS.—The Secretary of Homeland Security is authorized to award grants to eligible entities to develop an improved seal for cargo containers that—

(A) permit the immediate detection of tampering with the seal;

(B) permit the immediate detection of tampering with the walls, ceiling, or floor of a container that indicates a person is attempting to improperly access the container; and

(C) transmit information regarding tampering with the seal, walls, ceiling, or floor of the container in real time to the appropriate authorities at a remote location.

(2) APPLICATION.—Each eligible entity seeking a grant under this subsection shall submit an application to the Secretary at such time, in such manner, and accompanied by such information as the Secretary may reasonably require.

(3) ELIGIBLE ENTITY.—In this subsection, the term “eligible entity” means any national laboratory, nonprofit private organization, institution of higher education, or other entity that the Secretary determines is eligible to receive a grant authorized by paragraph (1).

(d) EMPTY CONTAINERS.—

(1) CERTIFICATION.—The Secretary of Homeland Security shall prescribe in regulations requirements for certification of empty containers that are to be shipped to or from

the United States either directly or via a foreign port. Such regulations shall require that an empty container—

(A) be inspected and certified as empty prior to being loaded onto a vessel for transportation to a United States seaport; and

(B) be sealed with a high security container seal approved under subsection (a)(1) to enhance the security of United States seaports.

#### SEC. 235. OFFICE AND INSPECTION FACILITIES.

(a) OPERATIONAL SPACE IN SEAPORTS.—Each entity that owns or operates a United States seaport that receives cargo from a foreign country, whether governmental, quasi-governmental, or private, shall provide to the Directorate permanent office and inspection space within the seaport that is sufficient for the Directorate officers at the seaport to carry out their responsibilities. Such office and inspection space—

(1) shall be provided at no cost to the Directorate; and

(2) may be located outside the terminal area of the seaport.

(b) INSPECTION TECHNOLOGY.—The Secretary of Homeland Security shall maintain permanent inspection facilities that utilize available inspection technology in the space provided at each seaport pursuant to subsection (a).

#### SEC. 236. SECURITY GRANTS TO SEAPORTS.

(a) CRITERIA FOR AWARDED GRANTS.—Notwithstanding any other provision of law, the Secretary of Homeland Security shall use the proportion of the containerized imports that are received at a United States seaport as a factor to be considered when determining whether to select that seaport for award of a competitive grant for security.

(b) DEFINITIONS.—In this section:

(1) CONTAINERIZED IMPORTS.—The term “containerized imports” means the number of twenty-foot equivalent units of containerized imports that enter the United States annually through a United States seaport as estimated by the Bureau of Transportation Statistics of the Department of Transportation.

(2) COMPETITIVE GRANT FOR SECURITY.—The term “competitive grant for security” means a grant of Federal financial assistance that the Secretary of Homeland Security is authorized to award to a United States seaport for the purpose of enhancing security at the seaport, including a grant of funds appropriated under the heading “Maritime and Land Security” in title I of division I of the Consolidated Appropriations Resolution, 2003 (Public Law 108-7).

### TITLE III—AUTHORIZATION

#### SEC. 301. AUTHORIZATION OF APPROPRIATIONS.

There are authorized to be appropriated to the Attorney General and the Secretary of Homeland Security such sums as are necessary to carry out this Act. Sums authorized to be appropriated under this section are authorized to remain available until expended.

### SUBMITTED RESOLUTIONS

SENATE RESOLUTION 101—CALLING FOR THE PROSECUTION OF IRAQIS AND THEIR SUPPORTERS FOR WAR CRIMES, AND FOR OTHER PURPOSES

Mr. SPECTER submitted the following resolution; which was referred to the Committee on Foreign Relations:

S. RES. 101

*Resolved*, That it is the sense of the Senate that—