FOWLER, Mr. BAKER of California, Mr. OBERSTAR, Mr. CLEMENT, and Mr. POSHARD.

From the Committee on the Judiciary, for consideration of section 901 of the Senate bill, and section 430 of the House amendment, and modifications committed to the conference: Mr. HYDE, Mr. MCCOLLUM, and Mr. CONYERS.

EXECUTIVE AND OTHER COMMUNICATIONS

The following communications were laid before the Senate, together with accompanying papers, reports, and documents, which were referred as indicated:

EC–1909. A communication from the Secretary of Housing and Urban Development, transmitting pursuant to law, the semiannual reports for the period April 1 through September 30, 1995; to the Committee on Banking, Housing, and Urban Affairs.

EC–1910. A communication from the President and Chairman of the Export-Import Bank, transmitting, pursuant to law, a statement regarding a transaction involving exports to Ghana; to the Committee on Banking, Housing, and Urban Affairs.

EC–1911. A communication from the President and Chairman of the Export-Import Bank, transmitting, pursuant to law, a statement regarding a transaction involving exports to Indonesia; to the Committee on Banking, Housing, and Urban Affairs.

EC–1912. A communication from the Chairman of the Board of Governors of the Federal Reserve System, transmitting, pursuant to law, the Monetary Policy Report; to the Committee on Banking, Housing, and Urban Affairs.

EC–1913. A communication from the Managing Director of the Federal Housing Finance Board, transmitting, pursuant to law, the report of salary ranges for graded employees for calendar year 1996; to the Committee on Banking, Housing, and Urban Affairs.

EC–1914. A communication from the Acting Chairman of the Thrift Depositor Protection Oversight Board, transmitting, pursuant to law, the semi-annual report of the Office of the Inspector General for the period October 1 through December 31, 1995; to the Committee on Banking, Housing, and Urban Affairs.

REPORTS OF COMMITTEES

The following reports of committees were submitted:

By Mr. HATCH, from the Committee on the Judiciary, with an amendment in the nature of a substitute:

H.R. 782. A bill to amend title 18 of the United States Code to allow members of employee associations to represent their views before the United States Government.

By Mr. HATCH, from the Committee on the Judiciary, without amendment and with a preamble:

S. Res. 219. A resolution designating March 25, 1996 as ''Greek Independence Day: A National Day of Celebration of Greek and American Democracy.''

INTRODUCTION OF BILLS AND JOINT RESOLUTIONS

The following bills and joint resolutions were introduced, read the first and second time by unanimous consent, and referred as indicated:

By Mr. AKAKA:

S. 1585. A bill to authorize award of a medal to civilians who participated in the defense of Pearl Harbor and other military installations in Hawaii against attack by the Japanese on December 7, 1941; to the Committee on Armed Services.

By Mr. COHEN (for himself and Ms. SNOWE):

S. 1586. A bill for the relief of Nancy B. Wilson; to the Committee on Finance.

By Mr. LEAHY (for himself, Mr. BURNS, Mr. DOLE, Mr. PRESSLER, and Mrs. MURRAY):

S. 1587. A bill to affirm the rights of Americans to use and sell encryption products, to establish privacy standards for voluntary escrowed systems, and for other purposes; to the Committee on the Judiciary.

By Mr. STEVENS:

S. 1588. A bill to authorize the Secretary of Transportation to issue a certificate of documentation and coastwise trade endorsement for the vessel *Kalypso;* to the Committee on Commerce, Science, and Transportation.

By Mr. GORTON (for himself and Mr. LIEBERMAN):

S. 1589. A bill to provide for a rotating schedule for regional primaries for Presidential elections, and for other purposes; to the Committee on Rules and Administration.

By Mrs. MURRAY (for herself, Mr. LEAHY, Mr. BAUCUS, Mr. BUMPERS, and Mrs. FEINSTEIN):

S. 1590. A bill to repeal the emergency salvage timber sale program, and for other purposes; to the Committee on Energy and Natural Resources.

By Mr. D'AMATO:

S.J. Res. 50. A joint resolution to disapprove the certification of the President under section 490(b) of the Foreign Assistance Act of 1961 regarding foreign assistance for Mexico during fiscal year 1996; to the Committee on Foreign Relations.

STATEMENTS ON INTRODUCED BILLS AND JOINT RESOLUTIONS

By Mr. LEAHY (for himself, Mr. BURNS, Mr. DOLE, Mr. PRESSLER, and Mrs. MURRAY):

S. 1587. A bill to affirm the rights of Americans to use and sell encryption products, to establish privacy standards for voluntary escrowed systems, and for other purposes; to the Committee on the Judiciary.

THE ENCRYPTED COMMUNICATIONS PRIVACY ACT OF 1996

Mr. LEAHY. Mr. President, I am joined today by Senators BURNS, DOLE, PRESSLER, and MURRAY in introducing a bill that is pro-business, pro-jobs and pro-privacy.

The Encrypted Communications Privacy Act of 1996 would enhance the global competitiveness of our high-technology industries, protect the high-paying good jobs in those industries and maximize the choices in encryption technology available for businesses and individuals to protect the privacy, confidentiality and security of their computer, telephone, and other wire and electronic communications.

The guiding principle for this bill can be summed up in one sentence: Encryption is good for American business and good business for Americans.

FBI Director Louis Freeh testified last week at a hearing on economic espionage and quoted Secretary of State Warren Christopher as saying that ''Our national security is inseparable from our economic security.'' I could not agree more. Yet, American businesses are suffering a double blow from our current encryption policies. First, American firms lose billions of dollars each year due to the theft of proprietary economic information, which could be better protected if strong encryption were more widely used. Second, government export restrictions tie the hands of American high-technology businesses by barring the export of strong encryption technology. The size of these combined losses makes encryption one of the critical issues facing American businesses today.

Moreover, the increasing use of and dependency on networked computers by Americans to obtain critical medical services, to conduct research, to be entertained, to go shopping and to communicate with friends and business associates, raises special concerns about the privacy and confidentiality of their computer transmissions. I have long been concerned about these issues, and have worked over the past decade to create a legal structure to foster privacy and security for our wire and electronic communications. Encryption technology provides an effective way to ensure that only the people we choose can read our communications.

A leading encryption expert, Matt Blaze, told me in a recent letter that our current regulations governing the use and export of encryption are having a ''deleterious effect on our country's ability to develop a reliable and trustworthy information infrastructure.'' It is time for Congress to take steps to put our national encryption policy on the right course.

The Encrypted Communications Privacy Act would accomplish three goals:

First, the bill encourages the use of encryption by legislatively confirming that Americans have the freedom to use and sell here in the United States any encryption technology that they feel is most appropriate to meet their privacy and security needs. The bill bars any government-mandated use of any particular encryption system, such as a key escrow encryption system.

Second, for those Americans who choose to use a key escrow encryption method, the bill establishes privacy standards for key holders and stringent procedures for how law enforcement can obtain access to decoding keys and decryption assistance. These standards would subject key holders to criminal and civil liability if they released the keys or divulged the identity and information about the user of the encryption system, without legal authorization. Commenting on these provisions, Bruce Schneir, who has literally written the textbook on encryption, said in a recent letter to me that the bill ''recognizes the special obligations of keyholders to be vigilant in safeguarding the information entrusted to them, without imposing hurtles on the use of cryptography.''

Finally, the bill loosens export restrictions on encryption products. Under the bill, it would be lawful for American companies to export high-technology products with encryption capabilities when comparable encryption capabilities are available from foreign suppliers, and generally available encryption software, including mass market products and encryption that is in the public domain. According to Mr. Schneir, the bill ''removes the strangle-hold that has encumbered the development of mass-market security solutions'' which are so vital to the development of our information infrastructure.

Senator MURRAY took a leading role in the last Congress on reforming our export restrictions on encryption, and I commend her for continuing to give this important issue her committed attention again in this Congress.

Current export restrictions allow the export of primarily weak encryption software programs. So weak, in fact, that a January 1996 report by an ad hoc group of world-renowned cryptographers and computer scientists estimated that it would take a pedestrian hacker a matter of hours to break and a foreign intelligence agency a matter of nanoseconds to break. No wonder that foreign buyers of encryption products are increasingly looking elsewhere for strong security. This hurts the competitiveness of our high-technology industry.

A recent report by the Computer Systems Policy Project, which is a group of major American computer companies estimated that U.S. companies stand to lose between $30 and $60 billion in revenues and over 200,000 of high-technology jobs by the year 2000 because U.S. companies are handicapped in the global market by outdated export restrictions.

Even the Commerce Department reported in January that U.S. export controls may have a ''negative effect on U.S. competitiveness'' and ''may discourage'' the use of strong encryption domestically since manufacturers want to make only one product for export and for use here.

Although American companies account for almost 75 percent of the global market for prepackaged software, the rest of the world is competing strongly in the market for encryption software. Shortsighted government policy is holding back American business. Almost 2 years ago, I chaired a hearing of the Judiciary Subcommittee on Technology and the Law on the administration's Clipper Chip key escrow encryption program. I heard testimony about 340 foreign encryption products that were available worldwide, 155 of them employing encryption in a strength that American firms were prohibited from exporting.

In 2 short years, those numbers have increased. According to a survey of cryptographic products conducted by Trusted Information System, as of December 1995, 497 foreign products from 28 countries were available with encryption security. Almost 200 of these foreign products used strong encryption that American companies are barred from selling abroad. This study draws the obvious conclusion that ''As a result, U.S. Government restrictions may be succeeding only in crippling a vital American industry's exporting ability.''

At the Clipper Chip hearing I chaired in 1994, I heard a number of reports about American companies losing business opportunities due to U.S. export restrictions. One data security company reported that despite its superior system, it had been unable to respond to requests from NATO and foreign telecommunications companies because it cannot export the encryption they demanded. This cost this single American company millions in foregone business. Another major computer company lost two sales in Western Europe in a single year totaling about $80 million because the file and data encryption in the integrated system they offered was not exportable.

Our current export restrictions on encryption technology are fencing off the global marketplace and hurting the competitiveness of this part of our high-technology industries. While national and domestic security concerns must weigh heavily, we need to do a better job of balancing these concerns with American business' need for encryption and the economic opportunities for our high-technology industries that encryption technology provides.

American businesses are not only suffering lost sales because of our current export restrictions, but are also suffering staggering losses due to economic espionage. FBI Director Freeh testified that the White House Office of Science and Technology Policy puts the amount of that loss at $100 billion per year. At a hearing last week on economic espionage, we heard from one witness who had to close down his software company, with a loss of 25 jobs, after China bribed an employee to steal the source code for the company's software.

We have bills pending before Congress to enact new criminal laws to punish people who steal trade secrets or other proprietary information and who break into computers to steal sensitive information. But new criminal laws are not the whole answer. Criminal laws often only come into play too late, after the theft has occurred or the injury inflicted.

We must encourage American firms to take preventive measures to protect their vital economic information. That is where encryption comes in. Just as we have security systems to lock up our offices and file drawers, we need strong encryption systems to protect the security and confidentiality of business information.

The Computer Systems Policy Project estimates that, without strong encryption, financial losses by the year 2000 from breaches of computer security systems to be from $40 to $80 billion. Unfortunately, some of these losses are already occurring. One U.S.-based manufacturer is quoted in the Project's report, saying:

> We had a multi-year, multi-billion dollar contract stolen off our P.C. (while bidding in a foreign country). Had it been encrypted, [the foreign competitor] could not have used it in the bidding time frame.

New technologies present enormous opportunities for Americans, but we must strive to safeguard our privacy if these technologies are to prosper in this information age. Otherwise, in the service of law enforcement and intelligence needs, we will dampen any enthusiasm Americans may have for taking advantage of the new technologies.

I look forward to working with my colleagues on this important matter, and ask unanimous consent that the bill, a summary of the bill, and three letters of support from Matt Blaze, Bruce Schneir, and Business Software Alliance, be included in the RECORD.

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

S. 1587

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

SECTION 1. SHORT TITLE.

This Act may be cited as the ''Encrypted Communications Privacy Act of 1996''.

SEC. 2. PURPOSE.

It is the purpose of this Act—

(1) to ensure that Americans are able to have the maximum possible choice in encryption methods to protect the security, confidentiality, and privacy of their lawful wire or electronic communications; and

(2) to establish privacy standards for key holders who are voluntarily entrusted with the means to decrypt such communications, and procedures by which investigative or law enforcement officers may obtain assistance in decrypting such communications.

SEC. 3. FINDINGS.

The Congress finds that—

(1) the digitization of information and the explosion in the growth of computing and electronic networking offers tremendous potential benefits to the way Americans live, work, and are entertained, but also raises new threats to the privacy of American citizens and the competitiveness of American businesses;

(2) a secure, private, and trusted national and global information infrastructure is essential to promote economic growth, protect citizens' privacy, and meet the needs of American citizens and businesses;

(3) the rights of Americans to the privacy and security of their communications and in conducting their personal and business affairs should be preserved and protected;

(4) the authority and ability of investigative and law enforcement officers to access and decipher, in a timely manner and as provided by law, wire and electronic communications necessary to provide for public safety and national security should also be preserved;

(5) individuals will not entrust their sensitive personal, medical, financial, and other information to computers and computer networks unless the security and privacy of that information is assured;

(6) business will not entrust their proprietary and sensitive corporate information,

including information about products, processes, customers, finances, and employees, to computers and computer networks unless the security and privacy of that information is assured;

(7) encryption technology can enhance the privacy, security, confidentiality, integrity, and authenticity of wire and electronic communications and stored electronic information;

(8) encryption techniques, technology, programs, and products are widely available worldwide;

(9) Americans should be free lawfully to use whatever particular encryption techniques, technologies, programs, or products developed in the marketplace they desire in order to interact electronically worldwide in a secure, private, and confidential manner;

(10) American companies should be free to compete and to sell encryption technology, programs, and products;

(11) there is a need to develop a national encryption policy that advances the development of the national and global information infrastructure, and preserves Americans' right to privacy and the Nation's public safety and national security;

(12) there is a need to clarify the legal rights and responsibilities of key holders who are voluntarily entrusted with the means to decrypt wire or electronic communications;

(13) the Congress and the American people have recognized the need to balance the right to privacy and the protection of the public safety and national security;

(14) the Congress has permitted lawful electronic surveillance by investigative or law enforcement officers only upon compliance with stringent statutory standards and procedures; and

(15) there is a need to clarify the standards and procedures by which investigative or law enforcement officers obtain assistance from key holders who are voluntarily entrusted with the means to decrypt wire or electronic communications, including such communications in electronic storage.

SEC. 4. FREEDOM TO USE ENCRYPTION.

(a) LAWFUL USE OF ENCRYPTION.—It shall be lawful for any person within any State of the United States, the District of Columbia, the Commonwealth of Puerto Rico, and any territory or possession of the United States, and by United States persons in a foreign country to use any encryption, regardless of encryption algorithm selected, encryption key length chosen, or implementation technique or medium used except as provided in this Act and the amendments made by this Act or in any other law.

(b) GENERAL CONSTRUCTION.—Nothing in this Act or the amendments made by this Act shall be construed to—

(1) require the use by any person of any form of encryption;

(2) limit or affect the ability of any person to use encryption without a key escrow function; or

(3) limit or affect the ability of any person who chooses to use encryption with a key escrow function not to use a key holder.

SEC. 5. ENCRYPTED WIRE AND ELECTRONIC COMMUNICATIONS.

(a) IN GENERAL.—Part I of title 18, United States Code, is amended by inserting after chapter 121 the following new chapter:

"CHAPTER 122—ENCRYPTED WIRE AND ELECTRONIC COMMUNICATIONS

"§ 2801. Definitions

''As used in this chapter—

''(1) the terms 'person', 'State', 'wire communication', 'electronic communication', 'investigative or law enforcement officer', 'judge of competent jurisdiction', and 'electronic storage' have the same meanings given such terms in section 2510 of this title;

''(2) the term 'encryption' means the scrambling of wire or electronic communications using mathematical formulas or algorithms in order to preserve the confidentiality, integrity or authenticity and prevent unauthorized recipients from accessing or altering such communications;

''(3) the term 'key holder' means a person located within the United States (which may, but is not required to, be a Federal agency) who is voluntarily entrusted by another independent person with the means to decrypt that person's wire or electronic communications for the purpose of subsequent decryption of such communications;

''(4) the term 'decryption key' means the variable information used in a mathematical formula, code, or algorithm, or any component thereof, used to decrypt wire or electronic communications that have been encrypted; and

''(5) the term 'decryption assistance' means providing access, to the extent possible, to the plain text of encrypted wire or electronic communications.

"§ 2802. Prohibited acts by key holders

''(a) UNAUTHORIZED RELEASE OF KEY.—Except as provided in subsection (b), any key holder who releases a decryption key or provides decryption assistance shall be subject to the criminal penalties provided in subsection (e) and to civil liability as provided in subsection (f).

''(b) AUTHORIZED RELEASE OF KEY.—A key holder shall only release a decryption key in its possession or control or provide decryption assistance—

''(1) with the lawful consent of the person whose key is being held or managed by the key holder;

''(2) as may be necessarily incident to the holding or management of the key by the key holder; or

''(3) to investigative or law enforcement officers authorized by law to intercept wire or electronic communications under chapter 119, to obtain access to stored wire and electronic communications and transactional records under chapter 121, or to conduct electronic surveillance, as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801), upon compliance with subsection (c) of this section.

''(c) REQUIREMENTS FOR RELEASE OF DECRYPTION KEY OR PROVISION OF DECRYPTION ASSISTANCE TO INVESTIGATIVE OR LAW ENFORCEMENT OFFICER.—

''(1) CONTENTS OF WIRE AND ELECTRONIC COMMUNICATIONS.—A key holder is authorized to release a decryption key or provide decryption assistance to an investigative or law enforcement officer authorized by law to conduct electronic surveillance under chapter 119, only if—

''(A) the key holder is given—

''(i) a court order signed by a judge of competent jurisdiction directing such release or assistance; or

''(ii) a certification in writing by a person specified in section 2518(7) or the Attorney General stating that—

''(I) no warrant or court order is required by law;

''(II) all requirements under section 2518(7) have been met; and

''(III) the specified release or assistance is required;

''(B) the order or certification under paragraph (A)—

''(i) specifies the decryption key or decryption assistance which is being sought; and

''(ii) identifies the termination date of the period for which release or assistance has been authorized; and

''(C) in compliance with an order or certification under subparagraph (A), the key holder shall provide only such key release or decryption assistance as is necessary for access to communications covered by subparagraph (B).

''(2) STORED WIRE AND ELECTRONIC COMMUNICATIONS.—(A) A key holder is authorized to release a decryption key or provide decryption assistance to an investigative or law enforcement officer authorized by law to obtain access to stored wire and electronic communications and transactional records under chapter 121, only if the key holder is directed to give such assistance pursuant to the same lawful process (court warrant, order, subpoena, or certification) used to obtain access to the stored wire and electronic communications and transactional records.

''(B) The notification required under section 2703(b) shall, in the event that encrypted wire or electronic communications were obtained from electronic storage, include notice of the fact that a key to such communications was or was not released or decryption assistance was or was not provided by a key holder.

''(C) In compliance with the lawful process under subparagraph (A), the key holder shall provide only such key release or decryption assistance as is necessary for access to the communications covered by such lawful process.

''(3) USE OF KEY.—(A) An investigative or law enforcement officer to whom a key has been released under this subsection may use the key only in the manner and for the purpose and duration that is expressly provided for in the court order or other provision of law authorizing such release and use, not to exceed the duration of the electronic surveillance for which the key was released.

''(B) On or before completion of the authorized release period, the investigative or law enforcement officer to whom a key has been released shall destroy and not retain the released key.

''(C) The inventory required to be served pursuant to section 2518(8)(d) on persons named in the order or the application under section 2518(7)(b), and such other parties to intercepted communications as the judge may determine, in the interest of justice, shall, in the event that encrypted wire or electronic communications were intercepted, include notice of the fact that during the period of the order or extensions thereof a key to, or decryption assistance for, any encrypted wire or electronic communications of the person or party intercepted was or was not provided by a key holder.

''(4) NONDISCLOSURE OF RELEASE.—No key holder, officer, employee, or agent thereof shall disclose the key release or provision of decryption assistance pursuant to subsection (b), except as may otherwise be required by legal process and then only after prior notification to the Attorney General or to the principal prosecuting attorney of a State or any political subdivision of a State, as may be appropriate.

''(d) RECORDS OR OTHER INFORMATION HELD BY KEY HOLDERS.—A key holder, shall not disclose a record or other information (not including the key) pertaining to any person whose key is being held or managed by the key holder, except—

''(1) with the lawful consent of the person whose key is being held or managed by the key holder; or

''(2) to an investigative or law enforcement officer pursuant to a subpoena authorized

under Federal or State law, court order, or lawful process.

An investigative or law enforcement officer receiving a record or information under paragraph (2) is not required to provide notice to the person to whom the record or information pertains. Any disclosure in violation of this subsection shall render the person committing the violation liable for the civil damages provided for in subsection (f).

''(e) CRIMINAL PENALTIES.—The punishment for an offense under subsection (a) of this section is—

''(1) if the offense is committed for a tortious, malicious, or illegal purpose, or for purposes of direct or indirect commercial advantage or private commercial gain—

''(A) a fine under this title or imprisonment for not more than 1 year, or both, in the case of a first offense under this subparagraph; or

''(B) a fine under this title or imprisonment for not more than 2 years, or both, for any second or subsequent offense; and

''(2) in any other case where the offense is committed recklessly or intentionally, a fine of not more than $5,000 or imprisonment for not more than 6 months, or both.

''(f) CIVIL DAMAGES.—

''(1) IN GENERAL.—Any person aggrieved by any act of a person in violation of subsections (a) or (d) may in a civil action recover from such person appropriate relief.

''(2) RELIEF.—In an action under this subsection, appropriate relief includes—

''(A) such preliminary and other equitable or declaratory relief as may be appropriate;

''(B) damages under paragraph (3) and punitive damages in appropriate cases; and

''(C) a reasonable attorney's fee and other litigation costs reasonably incurred.

''(3) COMPUTATION OF DAMAGES.—The court may assess as damages whichever is the greater of—

''(A) the sum of the actual damages suffered by the plaintiff and any profits made by the violator as a result of the violation; or

''(B) statutory damages in the amount of $5,000.

''(4) LIMITATION.—A civil action under this subsection shall not be commenced later than 2 years after the date upon which the plaintiff first knew or should have known of the violation.

''(g) DEFENSE.—It shall be a complete defense against any civil or criminal action brought under this chapter that the defendant acted in good faith reliance upon a court warrant or order, grand jury or trial subpoena, or statutory authorization.

''§ 2803. Reporting requirements

''(a) IN GENERAL.—In reporting to the Administrative Office of the United States Courts as required under section 2519(2) of this title, the Attorney General, an Assistant Attorney General specially designated by the Attorney General, the principal prosecuting attorney of a State, or the principal prosecuting attorney of any political subdivision of a State, shall report on the number of orders and extensions served on key holders to obtain access to decryption keys or decryption assistance.

''(b) REQUIREMENTS.—The Director of the Administrative Office of the United States Courts shall include as part of the report transmitted to the Congress under section 2519(3) of this title, the number of orders and extensions served on key holders to obtain access to decryption keys or decryption assistance and the offenses for which the orders were obtained.

''§ 2804. Unlawful use of encryption to obstruct justice

''Whoever willfully endeavors by means of encryption to obstruct, impede, or prevent the communication of information in furtherance of a felony which may be prosecuted in a court of the United States, to an investigative or law enforcement officer shall—

''(1) in the case of a first conviction, be sentenced to imprisonment for not more than 5 years, fined under this title, or both; or

''(2) in the case of a second or subsequent conviction, be sentenced to imprisonment for not more than 10 years, fined under this title, or both.

''§ 2805. Freedom to sell encryption products

''(a) IN GENERAL.—It shall be lawful for any person within any State of the United States, the District of Columbia, the Commonwealth of Puerto Rico, and any territory or possession of the United States, to sell in interstate commerce any encryption, regardless of encryption algorithm selected, encryption key length chosen, or implementation technique or medium used.

''(b) CONTROL OF EXPORTS BY SECRETARY OF COMMERCE.—

''(1) GENERAL RULE.—Notwithstanding any other law, subject to paragraphs (2), (3), and (4), the Secretary of Commerce shall have exclusive authority to control exports of all computer hardware, software, and technology for information security (including encryption), except computer hardware, software, and technology that is specifically designed or modified for military use, including command, control, and intelligence applications.

''(2) ITEMS NOT REQUIRING LICENSES.—No validated license may be required, except pursuant to the Trading With The Enemy Act or the International Emergency Economic Powers Act (IEEPA) (but only to the extent that the authority of the IEEPA is not exercised to extend controls imposed under the Export Administration Act of 1979), for the export or reexport of—

''(A) any software, including software with encryption capabilities, that is—

''(i) generally available, as is, and designed for installation by the purchaser; or

''(ii) in the public domain or publicly available because it is generally accessible to the interested public in any form; or

''(B) any computing device solely because it incorporates or employs in any form software (including software with encryption capabilities) exempted from any requirement for a validated license under subparagraph (A).

''(3) SOFTWARE WITH ENCRYPTION CAPABILITIES.—The Secretary of Commerce shall authorize the export or reexport of software with encryption capabilities for nonmilitary end-uses in any country to which exports of software of similar capability are permitted for use by financial institutions not controlled in fact by United States persons, unless there is substantial evidence that such software will be—

''(A) diverted to a military end-use or an end-use supporting international terrorism;

''(B) modified for military or terrorist end-use; or

''(C) reexported without requisite United States authorization.

''(4) HARDWARE WITH ENCRYPTION CAPABILITIES.—The Secretary shall authorize the export or reexport of computer hardware with encryption capabilities if the Secretary determines that a product offering comparable security is commercially available from a foreign supplier without effective restrictions outside the United States.

''(5) DEFINITIONS.—As used in this subsection—

''(A) the term 'generally available' means, in the case of software (including software with encryption capabilities), software that is widely offered for sale, license, or transfer including, but not limited to, over-the-counter retail sales, mail order transactions, phone order transactions, electronic distribution, or sale on approval;

''(B) the term 'as is' means, in the case of software (including software with encryption capabilities), a software program that is not designed, developed, or tailored by the software company for specific purchasers, except that such purchasers may supply certain installation parameters needed by the software program to function properly with the purchaser's system and may customize the software program by choosing among options contained in the software program;

''(C) the term 'is designed for installation by the purchaser' means, in the case of software (including software with encryption capabilities)—

''(i) the software company intends for the purchaser (including any licensee or transferee), who may not be the actual program user, to install the software program on a computing device and has supplied the necessary instructions to do so, except that the company may also provide telephone helpline services for software installation, electronic transmission, or basic operations; and

''(ii) that the software program is designed for installation by the purchaser without further substantial support by the supplier;

''(D) the term 'computing device' means a device which incorporates one or more microprocessor-based central processing units that can accept, store, process, or provide output of data; and

''(E) the term 'computer hardware', when used in conjunction with information security, includes, but is not limited to, computer systems, equipment, application-specific assemblies, modules, and integrated circuits.''.

(b) TECHNICAL AMENDMENT.—The table of chapters for part I of title 18, United States Code, is amended by inserting after the item relating to chapter 33, the following new item:

''122. Encrypted wire and electronic communications ..... 2801''.

SEC. 6. INTELLIGENCE ACTIVITIES.

(a) CONSTRUCTION.—Nothing in this Act or the amendments made by this Act constitutes authority for the conduct of any intelligence activity.

(b) CERTAIN CONDUCT.—Nothing in this Act or the amendments made by this Act shall affect the conduct, by officers or employees of the United States Government in accordance with other applicable Federal law, under procedures approved by the Attorney General, or activities intended to—

(1) intercept encrypted or other official communications of United States executive branch entities or United States Government contractors for communications security purposes;

(2) intercept radio communications transmitted between or among foreign powers or agents of a foreign power as defined by the Foreign Intelligence Surveillance Act of 1978; or

(3) access an electronic communication system used exclusively by a foreign power or agent of a foreign power as defined by the Foreign Intelligence Surveillance Act of 1978.

ENCRYPTED COMMUNICATIONS PRIVACY ACT OF 1996—SUMMARY

Sec. 1. Short Title. The Act many be cited as the ''Encrypted Communications Privacy Act of 1996.''

Sec. 2. Purpose. The Act would ensure that Americans have the maximum possible choice in encryption methods to protect the

security, confidentiality and privacy of their lawful wire and electronic communications. For those Americans who choose an encryption method in which another person, called a ''key holder,'' is voluntarily entrusted with the decryption key, the Act would establish privacy standards for the key holder, and procedures for law enforcement officers to follow to obtain assistance from the key holder in decrypting encrypted communications.

Sec. 3. Findings. The Act enumerates fifteen congressional findings, including that a secure, private and trusted national and global information infrastructure is essential to promote citizens' privacy and meet the needs of both American citizens and businesses, that encryption technology widely available worldwide can help meet those needs, that Americans should be free to use, and American businesses free to compete and sell, encryption technology, programs and products, and that there is a need to develop a national encryption policy to advance the global information infrastructure and preserve Americans' right to privacy and the Nation's public safety and national security.

Sec. 4. Freedom to Use Encryption

(a) Lawful Use of Encryption. The Act legislatively confirms current practice in the United States that any person in this country may lawfully use any encryption method, regardless of encryption algorithm, key length or implementation selected. The Act thereby prohibits any government-mandated use of any particular encryption system, such as a key escrow encryption system.

The Act further makes lawful the use of any encryption method by United States persons in a foreign country. This provision is consistent with, though broader than, the Department of State's new personal use exemption published in the Federal Register on February 16, 1996, that permits the export of cryptographic products by U.S. citizens and permanent residents who have the need to temporarily export the cryptographic products when leaving the U.S. for brief periods of time. For example, under this new exemption, U.S. citizens traveling abroad will be able to take their laptop computers containing copies of Lotus Notes software, many versions of which contain an encryption program otherwise not exportable.

(b) General Constructions. Nothing in the Act is to be construed to require the use of encryption, a key escrow encryption system, or a key holder if a person chooses to use a key escrow encryption system.

Sec. 5. Encrypted wire and electronic communications. This section of the Act adds a new chapter 122, entitled ''Encrypted Wire and Electronic Communications,'' to title 18 of the United States Code to establish privacy standards for key holders and to set forth procedures that law enforcement officers must follow to obtain decryption assistance from key holders.

(a) In General. New chapter 122 has five sections.

§ 2801. Definitions. Generally, the terms used in the new chapter have the same meanings as in the federal wiretap statute in 18 U.S.C. § 2510. Definitions are provided for ''encryption'', ''key holder'', ''decryption key'', and ''decryption assistance''. A ''key holder'' may, but is not required to be, a Federal agency.

This chapter applies only to wire or electronic communications and communications in electronic storage, as defined in 18 U.S.C. § 2510, and not to stored electronic data. For example, encrypted electronic mail messages, encrypted telephone conversations, encrypted facsimile transmissions, encrypted computer transmissions and encrypted file transfers over the Internet would be covered, but not encrypted data merely stored on computers.

§ 2802. Prohibited acts by key holders

(a) Unauthorized release of key.—Key holders will be subject to both criminal and civil liability for the unauthorized release of decryption keys or providing unauthorized decryption assistance.

(b) Authorized release of key.—Key holders are authorized to release decryption keys or provide decryption assistance with the consent of the key owner, as may be necessary for the holding or management of the key, or to investigative or law enforcement officers upon compliance with the procedures set forth in subsection (c).

(c) Requirements for release of decryption key to investigative or law enforcement officer.—To obtain access to a decryption key or decryption assistance from a key holder, an investigative or law enforcement officer must present to the key holder the same form of lawful process used to obtain access to the encrypted content. For example, to obtain the decryption key to, or decryption assistance for, an encrypted telephone conversation that is the subject of a court-ordered wiretap under 18 U.S.C. § 2518, a law enforcement agent must present a court order to the key holder to obtain the decoding key. Likewise, to obtain the decryption key to, or decryption assistance for, an encrypted stored wire or electronic communication, a law enforcement officer must present a court warrant, order, subpoena or certification, depending upon what process was used to obtain access to the stored communication.

Key holders may only provide the minimal key release or decryption assistance needed to access the particular communications specified by court order or other legal process. Released keys or other decryption assistance may only be used in the manner and for the purpose and duration expressly provided by court order or other legal process.

A key holder who fails to provide the decryption key or decryption assistance called for in the court order, subpoena or other lawful process may be penalized under current contempt or obstruction laws.

(d) Records or other information held by key holders.—Key holders are prohibited from disclosing records or other information (not including decryption keys) pertaining to key owners, except with the owner's consent or to an investigative or law enforcement officer, pursuant to a subpoena, court order or other lawful process.

(e) Criminal penalties.—Key holders who violate this section for a tortious, malicious or an illegal purpose, or for direct or indirect commercial advantage or private commercial gain, will be subject to a fine and up to 1 year imprisonment for a first offense, and fine and up to 2 years' imprisonment for a second offense. Other reckless and intentional violations would subject the key holder to a fine of up to $5,000 and up to 6 months' imprisonment.

(f) Civil damages.—Persons aggrieved by key holder violations may sue for injunctive relief, and actual damages or statutory damages of $5,000, whichever is greater.

(g) Defense.—A complete defense is provided if the defendant acted in good faith reliance upon a court order, warrant, grand jury or trial subpoena or statutory authorization.

§ 2803. Reporting requirements. The Attorney General is required to include in her report to the Administrative Office of the U.S. Courts under 18 U.S.C. § 2519(2), the number of orders and extensions served on key holders to obtain access to decryption keys or decryption assistance. The Director of the Administrative Office of the U.S. Courts is required to include this information, and the offenses for which the orders were obtained, in the report to Congress under 18 U.S.C. § 2519(3).

§ 2804. Unlawful use of encryption to obstruct justice. Persons who willfully use encryption in an effort and for the purpose of obstructing, impeding, or prevent the communication of information in furtherance of a federal felony crime to a law enforcement officer, would be subject to a fine and up to 5 years' imprisonment for a first offense, and up to 10 years' imprisonment for a second or subsequent offense.

§ 2805. Freedom to sell encryption products

(a) In general.—The Act, legislatively confirms that it is lawful to sell any encryption, regardless of encryption algorithm, key length or implementation used, domestically in the United States or its territories.

(b) Control of exports by Secretary of Commerce.—Notwithstanding any other law, the Act vests the Secretary of Commerce with control of exports of hardware, software and technology for information security, including encryption for both communications and other stored data, except when the hardware, software or technology is specifically designed or modified for military use.

No export license may be required for encryption software and hardware with encryption capabilities that is generally available, including mass market products (i.e., those generally available, sold ''as is'', and designed for installation by the purchaser) or encryption in the public domain and generally accessible. For example, no licenses would be required for encryption products commercially available without restriction and sold ''as is'', such as Netscape's commercially available World Wide Web Browser, which cannot be exported. Similarly, no license would be required to export software and corresponding hardware placed in the public domain and generally accessible, such as Phil Zimmerman's Pretty Good Privacy program, which has been distributed to the public free of charge via the Internet.

In addition, the Secretary of Commerce must authorize the export of encryption software to commercial users in any country to which exports of such software has been approved for use by foreign financial institutions, except when there is substantial evidence that the software will be diverted or modified for military or terrorists' end-use or re-exported without requisite U.S. authorization. Finally, the Secretary of Commerce must authorize the export of computer hardware with encryption capabilities if the Secretary determines that a product with comparable security is commercially available from foreign suppliers without effective restrictions outside the United States.

Significantly, the government is authorized to continue controls on countries that pose terrorism concerns, such as Libya, Syria and Iran, or other embargoes countries, such as Cuba and North Korea, pursuant to the Trading With the Enemy Act or the International Emergency Economic Powers Act.

(b) Technical Amendment. The Act adds new chapter 122 and the new title in the table of chapters in title 18 of the United States Code.

Sec. 6. Intelligence activities. The Act does not authorize the conduct of intelligence activities, nor affect the conduct by Federal government officers or employees in intercepting (1) encrypted or other official communications of Federal executive branch or Federal contractors for communications security purposes; (2) radio communications between or among foreign powers or agents, as defined by the Foreign Intelligence Surveillance Act (FISA); or (3) electronic communication systems used exclusively by foreign powers or agents, as defined by FISA.

MURRAY HILL, NJ,
March 1, 1996.

Hon. PATRICK LEAHY,
U.S. Senate.

DEAR SENATOR LEAHY: Thank you for introducing the Encrypted Communications Privacy Act of 1996. As a member of the computer security and cryptology research community, I have observed firsthand the deleterious effect that the current regulations governing the use and export of cryptography are having on our country's ability to develop a reliable and trustworthy information infrastructure. Your bill takes an important first step toward creating regulations that reflect the modern realities of this increasingly critical technology.

Unlike previous government encryption initiatives such as the technically-flawed and unworkable ''Clipper'' chip, your bill reaffirms the role of the marketplace in providing ordinary citizens and businesses with a full range of choices for securing their private information. In particular by freeing mass-market cryptographic software and hardware from the burdensome export controls that govern the international arms trade, the bill will help the American software industry compete, for the first time, in the international market for high-quality security products.

Law enforcement need not fear the widespread availability of encryption; indeed, they should welcome and promote it. Encryption thwarts electronic predators by preventing unauthorized access to private data and computer systems, and the use of strong cryptography to protect computer networks is becoming as natural and necessary as the use of locks and burglar alarms to protect our homes and businesses. While criminals, too, might occasionally derive some advantage from the use of cryptography, the benefits of widely-available encryption technology overwhelmingly favor the honest user. By recognizing that those who hold decryption keys on behalf of others are in a special position of trust, your bill is respectful of the privacy of law-abiding citizens without introducing impediments to the government's ability to investigate and prevent crime.

I have also examined the new provision designed to discourage the use of cryptography by criminals in the furtherance of a felony, and hope to see your carefully-worded language reinforced by a narrow interpretation in the courts, consistent with your intent.

Again, thank you for your continued leadership in this area, and I look forward to doing whatever I can to help you bring encryption regulations in line with the fast-changing reality of this emerging technology.

Sincerely,

MATT BLAZE.

March 1, 1996.

Hon. PATRICK LEAHY,
U.S. Senate.

DEAR SENATOR LEAHY. I would like to thank you for introducing the Encrypted Communications Privacy Act. As a member of the computer and information security research community, I am keenly aware of the vital role of cryptography in fostering the development of our information infrastructure.

As the author of the book, ''Applied Cryptography'', I have unusual insights into the absurdity of cryptography export restrictions. It is not without irony that one may export my book in paper format, but not electronically. Presumably no rational person believes that the current restrictions actually prevent the spread of cryptography. I believe you recognize this, as evidenced from the strong stance taken in your bill.

As the bill recognizes, we can no longer afford to hold on to the obsolete notion that cryptography is the sole province of government communications; the growth of modern networks has irrevocably pushed it into the mainstream. I applaud your leadership towards codifying these principles in a balanced and responsible way. In particular, the bill:

Removes the regulatory strangle-hold that has encumbered the development of mass-market security solutions; Recognizes the futility of applying regulations intended to control the international arms trade to even the most mundane and commonly available software; Encourages public confidence in encryption by allowing the marketplace to provide a full range of choices for privacy and security needs; Recognizes the special obligations of keyholders to be vigilant in safeguarding the information entrusted to them, without imposing hurtles on the use of cryptography; Allows the United States to continue its leadership role as a technological innovator; Acknowledges the pivotal role of cryptography in electronic commerce.

I continue to have concerns that the new criminal obstruction provision will discourage law abiding citizens from using cryptography. I hope that legislative history and further discussion will demonstrate the narrow intent of this crime.

Overall, your bill takes very necessary strides towards ensuring that the protections we take for granted in traditional media keep pace with technology, and I commend your efforts.

Sincerely,

BRUCE SCHNEIER.

BUSINESS SOFTWARE ALLIANCE,
Washington, DC, March 4, 1996,

Hon. PATRICK J. LEAHY,
Russell Senate Office Building,
Washington, DC.

DEAR SENATOR LEAHY: As President of the Business Software Alliance (BSA), I am writing to express our strong support for the Encryption Communications Privacy Act of 1996 which I understand you will introduce tomorrow. BSA represents the leading publishers of software for personal computers and the client server environment including Adobe, Autodesk, Bentley, Lotus Development, Microsoft, Novell, Sybase, Symantec and the Santa Cruz Operation.

We have had an opportunity to review the legislation and find it a significant step toward placing the U.S. software industry on a level playing field with our foreign competitors. Currently, we are only allowed to export weak (40-bit) encryption. Your legislation would allow us to export generally available software which offers security at prevailing world levels. While many would prefer export restrictions being lifted in their entirety, this legislation at least would place us on an equal footing with our foreign competitors which is critical to the continued success of the U.S. software industry in the global market place.

As you well know, today, America's software industry is the envy of the world. U.S. software companies hold an estimated 75% worldwide market share for mass market software with exports accounting for more than one-half of revenues for our companies. According to a 1993 study by Economists Inc., the American mass market software industry was the fastest growing industry in the U.S. between 1982 and 1992 and had become larger than all but five manufacturing industries. This translates into jobs here in the U.S.

The continued growth and success of our industry is directly threatened by existing U.S. government export controls. For that reason, our companies have consistently made this one of its top policy issues. As importantly, the availability of easy to use, affordable encryption will be essential to the successful development of the Global Information Infrastructure (GII). As more and more transactions are being done on-line, consumers are increasingly demanding software with strong encryption capabilities. In two studies, 90% of the respondents believe information security is important. In one study 37% of the respondents said that they would consider purchasing foreign software with otherwise less desirable features if that software offered data security not available in a U.S. program. Additionally, a recent study shows there are nearly 500 foreign encryption products from 28 countries currently available. U.S. export restrictions simply put U.S. industry at a competitive disadvantage. Your bill would address this issue by allowing U.S. industry to export generally available software with strong security features.

As you may know, the Administration has attempted to address this issue with a ''64-bit key escrow encryption proposal.'' Under that proposal, in order to be allowed to export software with strong security features, U.S. industry would be required to build a back door into the program with a spare key held by a U.S. government certified agent. After careful and serious deliberation by our members, we concluded that the Administration's approach is fatally flawed and cannot be the basis for progress in this area. We simply have not found a market for such a product. Any resolution must be market driven. Your bill takes a very different approach. It reaffirms Americans right to chose the encryption they use, either with key escrow or without. For those who chose voluntarily to use key holders, your legislation provides standards so that their privacy is not violated. Your legislation allows the market to work. We wholeheartedly endorse this market driven approach.

The digital information age and the Global Information Infrastructure present opportunities and challenges to computer users concerned about privacy at home and in their businesses, as well as for the U.S. government. From that point of view, we are all in a similar position. Information security policies for the electronic world are fundamental to the success of the GII and we are pleased to support your legislation which is pro-market, pro-competition, pro-privacy and pro-progress.

We look forward to working with you toward the enactment of this legislation.

Sincerely,

ROBERT W. HOLLEYMAN II,
President.

Mrs. MURRAY. Mr. President, I am pleased to join Senator LEAHY today as an original cosponsor of the Encrypted Communications Privacy Act. Senator LEAHY is truly a leader on this issue, and I've had the pleasure of working on encryption policy with him over the past 3 years. I'm excited to once again join him in this effort to make sense out of our national export control policies, and to promote export opportunities for American software and hardware producers.

As many of my colleagues know, with help from Congresswoman Cantwell in the 103d Congress, I was able to persuade the administration to study the extent to which U.S. companies are stymied by our country's current encryption and export control policies.

The Department of Commerce released that report last month. And let

me just say that there are some findings in this report that we should be aware of, and concerned about. For instance, the report acknowledges there are tremendous international growth opportunities for software exporters in the next 5 to 10 years. Unfortunately, the report also finds that most U.S. companies don't pursue international sales because our export control laws are too cost prohibitive.

Mr. President, there are legitimate national security concerns underpinning the Export Administration Act. However, these outdated laws are no longer relevant to the post-cold-war world we now lived in. Today's national security controls should target those items that really need to be controlled in order to maintain national security. Simply, they should make better sense; it doesn't make sense to tell a U.S. software producer they can't export a product that is already widely available on the world market.

Senator LEAHY'S bill seeks a balanced approach to implementing viable, safe, and secure encryption technology on both domestically sold products and exported products. It protects our privacy concerns, and it lays out the appropriate procedures law enforcement officials should use when obtaining encrypted materials. And, most important, it protects industry ingenuity and prohibits mandatory key escrow.

Mr. President, I introduced the Commercial Export Administration Act in the 103d Congress. I am pleased Senator LEAHY is incorporating my language into his bill. My language reduces regulatory redtape and makes it easier to export generally available mass-marketed commercial software. Washington State is home to some of the most innovative software producers in the world, and they are eager to export their goods. Unfortunately, our export controls keep Washington State's companies from penetrating the world market. Senator LEAHY'S bill, however will fix this problem.

We are hearing a lot on the Presidential campaign trail about the damage that comes from trade—how trade hurts our economy and our workers. That's nonsense. My Washington State friends and neighbors know full-well that trade is essential to our State's success. One out of every five jobs in Washington State is trade related; and these are highly skilled, family wage jobs that pay 15 percent higher than the national average. Moreover, Washington State's small- and mid-sized high-technology companies provided over 98,000 jobs in 1995.

Mr. President, I mention this because our bill will increase exports and enable our high-technology companies to grow further. Higher growth means more jobs—plain and simple. A recent study revealed that in 1995 U.S. exporters lost $60 billion in international sales, and it estimates the industry will lose 200,000 potential jobs by the year 2000. Given the increase in international competition, we can no longer afford to persist in holding U.S. companies back from potential world sales.

This legislation makes good sense. First and foremost, it ensures every American's right to use any appropriate encryption available on the market. It also sets out necessary guidelines that should accompany any policy regarding the use of key escrow. And finally, it paves the way for new, streamlined export policies.

Mr. President, this legislation is badly needed, and I urge my colleagues to join Senator LEAHY and me in supporting it.

By Mr. STEVENS:

S. 1588. A bill to authorize the Secretary of Transportation to issue a certificate of documentation and coastwise trade endorsement for the vessel *Kalypso;* to the Committee on Commerce, Science, and Transportation.

JONES ACT WAIVER LEGISLATION

• Mr. STEVENS. Mr. President, today I am introducing a bill to provide a certificate of documentation for the vessel *Kalypso*.

The *Kalypso* (vessel number 566349) is a 36-foot recreational vessel owned by Ronald Kent of Anchorage, AK. It was built in Largo, FL, in 1974. The vessel was apparently at one time owned by a non-U.S. citizen, and it is therefore ineligible for documentation under the Jones Act. Mr. Kent intends to use the vessel for charter fishing and sightseeing in Prince William Sound, AK.

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

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

S. 1588

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled, That notwithstanding sections 12106, 12107, and 12108 of title 46, United States Code, and section 27 of the Merchant Marine Act, 1920 (46 App. U.S.C. 883), as applicable on the date of enactment of this Act, the Secretary of Transportation may issue a certificate of documentation with appropriate endorsements for employment in the coastwise trade for the vessel Kalypso (vessel number 566349).•

By Mr. GORTON (for himself and Mr. LIEBERMAN):

S. 1589. A bill to provide for a rotating schedule for regional primaries for Presidential elections, and for other purposes; to the Committee on Rules and Administration.

THE PRESIDENTIAL PRIMARY ACT OF 1996

Mr. GORTON. Mr. President, reacting to a proposal which I am about to introduce in bill form, a columnist and cartoonist on the Seattle Post Intelligencer wrote, in yesterday's edition of that newspaper:

My English friend, Carolyn, having recently arrived in the United States from London, asked me to explain how Americans decide who will be their President.

We were at a social occasion just before I headed up to New Hampshire to witness the process firsthand. The longer I rambled on, detailing the haphazard series of primaries and caucuses, the influence of media expectations and money, the nearly endless campaigns that begin almost as soon as the winner of the previous round has been inaugurated, the more I thought how bizarre it must sound to a person from another country. . .

To the extent that the word ''system'' implies rationality and forethought, we really do not have a system for choosing nominees for president of the United States.

This bill also reflects a cartoon that this same individual had in the newspaper about 3 or 4 weeks ago. In that cartoon, several of the Founding Fathers, Benjamin Franklin, Thomas Jefferson, and Alexander Hamilton are ''Brainstorming at the Constitutional Convention.'' Ben Franklin turns to his colleagues in jest and rattles off an idea for a Presidential election system, with the following statement:

''The President shall be chosen from among those persons who can hone complex ideas into simplistic sound bites, defame the character of their opponents, hide their own blemishes from an intrusive swarming press corps and''—get this!—''win the most votes from a tiny number of citizens in a remote corner of New England!''

While this was simply a newspaper cartoon figure, it nonetheless comes all too close to describing the way in which we pick nominees for President of the United States at the present time.

A relatively small handful of voters in two or three States are wooed for more than a year while the rest of the country is ignored, and the influence of their votes, or even their sound bites on radio and on television, has a disproportionate impact on the way in which we nominate our Presidents. At the same time, it means that the candidates must have very narrow platforms, appealing to this not highly representative group of American citizens.

It also has the paradox, or had the paradox this year, of requiring major candidates to ignore States that somehow or another are deemed to be less influential. We saw an example this year when most of the candidates skipped primaries and caucuses in Louisiana and Delaware for fear of upsetting States that, for an extended period of time, had gone earlier than they did.

This is absolutely ridiculous, and we need a new and better system. We need a system that empowers and enfranchises all of the citizens of the United States equally; that treats the nominating process in both parties as being vitally important to the future of democratic institutions in the United States; that does so fairly; that causes the campaigns to speak about major national and regional issues on a much broader focus than they have at the present time. So, this is the time, it seems to me, when all of this is green in our memories, that we should begin the process toward a new system.

As a consequence, the bill that I am introducing today, together with my distinguished friend and colleague, the junior Senator from Connecticut [Mr. LIEBERMAN], creates a simple system of regional primaries. There will be four

regions, each including either 12 or 13 States, all required to hold primaries respectively on the first Tuesday in March—incidentally, today—the first Tuesday in April, and in May, and then in June, with the regions rotating first position, second position, third position, fourth position over four cycles, or 16 years. So the people in each region would go first once every four Presidential elections and last every fourth Presidential election.

The delegates would be bound for at least two ballots on the vote for the candidate to carry their State, or their congressional district, and leave the rules as to how the votes are divided to be determined by each individual State.

So the people of each State will have an equal opportunity to participate in and to influence the nomination in that process. Instead of 4 or 5 percent of the people of the United States having a disproportionate impact on the outcome, all of the people of the United States will have an equal opportunity, and, equally significant, the candidates for President will have had the campaign in all corners of the United States and in every State to be affected.

I believe, Mr. President, it will probably give a slightly greater advantage to those candidates who are not independently wealthy or do not have huge campaign chests because, with 12 or 13 primaries going on at the same time, they could attempt to establish a niche in one or two or three of those States and become well known, win one or two, and be major candidates by the time the second round comes around.

Not at all incidentally, Mr. President, it would place the nomination process a little bit closer to the national convention, and that perhaps would slightly shorten the entire process.

I think, in summary, Mr. President, that we should do everything we possibly can to improve the nomination system for President and see to it that all of our people have equal opportunity to participate.

Mr. President, I ask unanimous consent that a copy 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. 1589

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

SECTION 1. SHORT TITLE.

This Act may be cited as the ''Presidential Primary Act of 1996''.

SEC. 2. DEFINITION.

For purposes of this Act—

(1) the term ''election year'' means a year during which a Presidential election is to be held;

(2) the term ''national committee'' means the organization which, by virtue of the bylaws of a political party, is responsible for the day-to-day operation of such political party at the national level, as determined by the Federal Election Commission;

(3) the term ''political party'' means an association, committee, or organization which—

(A) nominates a candidate for election to any Federal office whose name appears on the election ballot as the candidate of such association, committee, or organization; and

(B) won electoral votes in the preceding Presidential election;

(4) the term ''primary'' means a primary election held for the selection of delegates to a national Presidential nominating convention of a political party, but does not include a caucus, convention, or other indirect means of selection; and

(5) the term ''State committee'' means the organization which, by virtue of the bylaws of a political party, is responsible for the day-to-day operation of such political party at the State level, as determined by the Federal Election Commission.

SEC. 3. SCHEDULE.

(a) SCHEDULE.—

(1) FIRST ELECTION CYCLE.—In the first election year after the date of enactment of this Act, each State shall hold a primary in accordance with this Act, according to the following schedule:

(A) REGION I.—Each State in Region I shall hold its primary on the first Tuesday in March.

(B) REGION II.—Each State in Region II shall hold its primary on the first Tuesday in April.

(C) REGION III.—Each State in Region III shall hold its primary on the first Tuesday in May.

(D) REGION IV.—Each State in Region IV shall hold its primary on the first Tuesday in June.

(2) SUBSEQUENT ELECTION CYCLES.—

(A) GENERAL RULE.—Except as provided in subparagraph (B), in the second and each subsequent election year after the date of enactment of this Act, each State in each region shall hold its primary on the first Tuesday of the month following the month in which it held its primary in the preceding election year.

(B) LIMITATION.—If the States in a region were required to hold their primaries not earlier than the first Tuesday in June of the preceding year, such States shall hold their primaries on the first Tuesday in March of the succeeding election year.

(b) REGIONS.—For purposes of subsection (a):

(1) REGION I.—Region I shall be comprised of the following:

(A) Connecticut.
(B) Delaware.
(C) District of Columbia.
(D) Maine.
(E) Maryland.
(F) Massachusetts.
(G) New Hampshire.
(H) New Jersey.
(I) New York.
(J) Pennsylvania.
(K) Rhode Island.
(L) Vermont.
(M) West Virginia.

(2) REGION II.—Region II shall be comprised of the following:

(A) Alabama.
(B) Arkansas.
(C) Florida.
(D) Georgia.
(E) Kentucky.
(F) Louisiana.
(G) Mississippi.
(H) North Carolina.
(I) Oklahoma.
(J) South Carolina.
(K) Tennessee.
(L) Texas.
(M) Virginia.

(3) REGION III.—Region III shall be comprised of the following:

(A) Illinois.
(B) Indiana.
(C) Iowa.
(D) Kansas.
(E) Michigan.
(F) Minnesota.
(G) Missouri.
(H) Nebraska.
(I) North Dakota.
(J) Ohio.
(K) South Dakota.
(L) Wisconsin.

(4) REGION IV.—Region IV shall be comprised of the following:

(A) Alaska.
(B) Arizona.
(C) California.
(D) Colorado.
(E) Hawaii.
(F) Idaho.
(G) Montana.
(H) Nevada.
(I) New Mexico.
(J) Oregon.
(K) Utah.
(L) Washington.
(M) Wyoming.

(5) TERRITORIES.—The national committees shall jointly determine the region of each territory of the United States.

SEC. 4. QUALIFICATION FOR BALLOT.

(a) CERTIFICATION BY FEDERAL ELECTION COMMISSION.—The Federal Election Commission shall certify to the States in the relevant region the names of all seriously considered candidates of each party—

(1) for the first primary in the election year, not later than 6 weeks before such primary; and

(2) in the subsequent primaries in the election year, not later than 1 week after the preceding primary in that election year.

(b) STATE PRIMARY BALLOTS.—Each State shall include on its primary ballot—

(1) the names certified by the Federal Election Commission; and

(2) any other names determined by the appropriate State committee.

SEC. 5. VOTING AT NATIONAL PARTY CONVENTIONS BY STATE DELEGATES.

(a) IN GENERAL.—Each State committee shall establish a procedure for the apportionment of delegates to the national Presidential nominating convention of each political party based on 1 of the following models:

(1) WINNER-TAKE-ALL.—A binding, winner-take-all system in which the results of the primary bind each member of the State delegation or Congressional district delegation (or combination thereof) to the national convention to cast his or her vote for the primary winner in the State.

(2) PROPORTIONATE PREFERENCE.—A binding proportionate representation system in which the results of the State primary are used to allocate members of the State delegation or Congressional district delegation (or combination thereof) to the national convention to Presidential candidates based on the proportion of the vote for some or all of the candidates received in the primary in the State.

(b) SELECTION OF DELEGATES.—

(1) SUBMISSION OF NAMES.—Not later than the date on which a candidate is certified on the ballot for a State, such candidate shall submit to the State committee, in priority order, a list of names of individuals proposed by the candidate to serve as delegates for such candidate.

(2) SELECTION.—Delegates apportioned to represent a candidate pursuant to the procedure established under subsection (a) shall be selected according to the list submitted by the candidate pursuant to paragraph (1).

(c) VOTING AT THE NATIONAL CONVENTIONS.—Each delegate to a national convention who is required to vote for the winner of the State primary under the system established under subsection (a) shall so vote for at least 2 ballots at the national convention, unless released by the winner of the State primary to which such delegate's vote is pledged.

SEC. 6. EFFECTIVE DATE.

This Act shall apply to the primaries in the year 2000 and in each election year thereafter.

By Mrs. MURRAY (for herself, Mr. LEAHY, Mr. BAUCUS, Mr. BUMPERS, and Mrs. FEINSTEIN):

S. 1590. A bill to repeal the emergency salvage timber sale program, and for other purposes; to the Committee on Energy and Natural Resources.

THE PUBLIC PARTICIPATION IN TIMBER SALVAGE ACT OF 1996

Mrs. MURRAY. Mr. President, I rise today to introduce legislation to correct serious problems with a law passed by this Congress at the beginning of last year. This law was intended to bypass environmental safeguards to speed up tree harvesting in national forests.

Mr. President, this law, commonly known as the salvage rider, has not worked. Instead, it has reopened old wounds in the Pacific Northwest, and sparked major controversy throughout the region. It has once again cast political uncertainty over working families, and blatantly cut regular people out of decisions over their own forests.

In short, what was billed as a commonsense approach to removing dead trees has turned out to be another case of legislative overkill on the environment.

Mr. President, it doesn't have to be this way. My bill will defuse a tense situation, provide certainty for workers, and restore a role for the public in forest management. Let me explain how.

The salvage rider has three problems: It allows large, old-growth timber sales previously declared illegal to be harvested without regard to fish and wildlife concerns; it could relegate the Northwest forest plan to the trash heap; and it cuts the public completely out of any final decision to harvest trees in national forests.

First, my bill resolves the old-growth issue by suspending timber sales commonly referred to as section 318 sales, and requiring the Forest Service to provide substitute timber volume or buy these sales back from the purchaser. In either case, the purchaser is held harmless, and so are the sensitive old-growth areas.

Second, my bill expedites implementation of the Northwest forest plan by making sure resources are available to complete recommended watershed analyses. The primary goal of this provision is to protect the scientific validity of option 9, so that timber sales can move ahead and private land owners can proceed with their habitat conservation plans.

This is a very important point: The State of Washington and every major timber land owner in the region are working on comprehensive habitat conservation plans. Every single one of these groups assume full implementation of option 9 as the basis of fish and wildlife protection in their own plans. If option 9 goes belly up, all of these habitat plans are worthless.

Third, my bill establishes a permanent, reasonable salvage program. The key work is permanent. I propose moving away from ad hoc forest planning by Congress, switching gears with every swing of the political pendulum. Instead, we should put a long-term program in place, something everyone can plan around, year in and year out.

Let me be very clear: This is not about salvage logging; this is about public input and accountability. Salvage logging is appropriate—and sometimes necessary—is done right. My bill sets up a program that allows the agencies to target salvage logging on an expedited basis when needed, under the full scrutiny of the public eye. If the agencies can defend their proposals, then they will go forward unimpeded.

Mr. President, I remember what it was like last spring. There was a new feeling in Congress; the people had called for change, so the leadership was running through bills left and right in the heat of the moment. A lot of things passed that might not have stood up under closer scrutiny, and this was one of them.

The irony here is thick: The salvage rider gave the Federal Government more power, and less accountability. As a result, the public has no say in how their own national forests are managed. I don't think the people wanted that kind of change.

People say this issue is too controversial to resolve, and that over the years it has become too polarized. To watch the debate, you might think that's true. Any person's idea is immediately rejected by someone else. And that may be the case with my bill. But if we keep rejecting everything, we will be left with nothing, except more chaos.

With all the controversy, people ask me, ''why bother?'' I'll tell you why: Because I care deeply about the Northwest. I care deeply about what government is saying to people about tough issues; more often than not, we're telling people that someone, somewhere, has to lose. That's not what I'm about. Most of all, I care deeply about the kind of legacy we're leaving for our children in this world.

We simply cannot continue the way of divide and conquer.

There are several ideas out there about how to proceed on this issue, from doing nothing at all, to repealing the salvage rider outright. My bill cuts a middle path. It says to workers: Salvage logging is something we should always be able to do. It says to conservationists: You will have an opportunity to hold the administration to its word. It says to large landowners: Your habitat planning efforts will pay off.

In my view, people ought to be willing to settle for this as a responsible approach.

Mr. President, I intend to pursue this matter on the continuing resolution when it comes before the full Senate. It is my understanding that the CR will contain limited language on this issue, but I do not believe it will solve the problem. I look forward to working with my colleagues.

Mr. President, I would also like to explain further some of the concepts contained in this bill.

REPLACEMENT VOLUME FOR SECTION 2001(K) SALES, SECTION 102(B)

The Secretary and contract holder/sale purchaser should immediately begin negotiations to locate alternative volume agreeable to both parties. Because these purchasers have owned these contracts for half a decade, the Secretary should make every effort to find and plan environmentally sound timber sales or modifications of the existing sale. The Secretary should direct agency personnel to make substitute volume a priority.

New sales or modifications of existing sales must comply with all applicable law, forest and regional plans, and standards and guidelines. Specifically, they must comply with the Northwest forest plan and, when developed, the plan—or plans—implementing the Interior Columbia Basin ecosystem management project. Furthermore, they must comply with Forest Service and BLM standards and guidelines, including PACFISH, INFISH, and Eastside screens.

BIDDING RIGHTS, SECTION 102(C)(2)

This bill contains provisions allowing for purchasers holding timber sale contracts for sales that do not comply with environmental or natural resource laws to exchange the value of those contracts for bidding credits. Such a concept has operated for mineral rights in at least two other natural resource laws—see Public Law 97–466, 96 Stat. 2540; and Public Law 96–401, 94 Stat. 1702.

This bill authorizes monetary credits based on the negotiated value of the purchaser's timber sale contract. The bidding credits extend to the purchaser and his or her successors and assigns to use in whole or part payment for future timber sales on Forest Service sales where the credits originated therefrom or on Bureau of Land Management sales, where the credits originated therefrom.

SALVAGE SALES INITIATED UNDER THE RIDER, SECTION 103(A)

Sales initiated under section 2001 (b) or (d) are all those begun since passage of the Emergency Timber Salvage Act, on July 27, 1995. Title III of this bill applies to sales where its provisions are timely. For example, if a sale has been advertised, this law does not require the agency to host an interdisciplinary team meeting with public participation. All sales that have not been awarded are subject to appeal under the provision of title III.

APPEAL OF AWARDED SALVAGE SALES, SECTION 103(B)

In section 103(b), I address sales that have been awarded to timber sale purchasers under the salvage and Northwest forest plan provisions of the rescissions bill. I give the public an opportunity to appeal immediately and thereby suspend sales that are causing environmental damage. The administration insists that it is complying with all environmental laws, and I want to give the public an opportunity to prove that is the case.

However, the agencies were required by the law at the time these sales were awarded—section 2001 of Public Law 104–19—to take procedural short cuts. I do not believe the purchasers should be denied their contract rights while the public challenges the agencies for obeying the law's procedural timelines. On the other hand, I do not want any sales that cause environmental harm to go forward. Thus, I try to strike a balance between these competing needs by limiting appeals to substantive complaints.

I understand that often substantive claims are raised in the context of procedural laws, such as the National Environmental Policy Act. Some courts have suggested that NEPA is a purely procedural statute. The term ''procedural'' in this bill is not meant to eliminate claims regarding environmental harm, even if they could be characterized as a purely procedural challenge. Let me give some examples.

Where an agency had documentation in which a biologist recommended a sale not go forward, but the agency allowed the sale to be awarded to a purchaser, then such documentation could be the basis for an appeal and would not be considered a procedural challenge. Another example would be where the agency went forward with a sale prior to obtaining the concurrence from the National Marine Fisheries Service or the U.S. Fish and Wildlife Service regarding whether an activity will or will not jeopardize a species under the Endangered Species Act. This should not be characterized as a procedural challenge. A final example would be that section 2001 of Public Law 109–14 required the agencies to, in their discretion, file only environmental assessments, not environmental impact statements. Because both EA's and EIS's should disclose the effects of a sale on the environment, a challenge could not be made simply because the agency published such information in an EA, rather than an EIS. However, if the documentation, no matter what its title, failed to disclose the effects on the environment, it would be open to challenge.

FUNDING TO IMPLEMENT TITLE III, SECTION 304

In this bill, the agencies are given discretion at the forest supervisor's and district manager's levels to combine several funds and accounts to implement this bill. The intent is to provide adequate funds for such activities as salvage timber sales, stewardship programs, watershed restoration, including road decommission, and data inventory and collection. This fund may not be used to carry out any activities that violate the forest plans, agency standards and guidelines, or the intent of this bill. This flexibility of funding will allow the agency to address critical salvage situations, correct an apparent agencywide problem with inadequate inventory of forest resources, and address a backlog of stewardship and restoration projects.

PILOT PROGRAM FOR HARVEST CONTRACTING, SECTION 306

The legislation authorizes a pilot program to change the way salvage timber sales are undertaken on Forest Service and BLM lands. The Forest Service currently sells timber by planning and preparing the sale, offering the sale to bidders, and administering the timber harvest. Harvest contracting or stewardship contracting is an alternative to the current method, entailing a two-step process: A timber harvest contract or contracts to cut and remove wood, and log sales from the collected and sorted wood.

There are several advantages to harvest contracting, including allowing the agencies to better implement ecosystem management, providing an opportunity to improve tree health without a large component of merchandise timber, eliminating below-cost timber sales, and reducing timber theft.

Specifically, harvest contracting would improve ecosystem management by basing contracts on the work performed and the resulting conditions of the forest. This would eliminate incentives for purchasers to inappropriately harvest large, lucrative trees. This pilot project encourages harvest so smaller, less valuable trees that have proliferated in many years of the West due to fire suppression and historic timber practices, such as highgrading. These young, dense stands are expensive to harvest, but many scientists believe it is important to remove them in order to restore health to timber stands.

The primary financial benefit is that gross timber sale revenues would be substantially higher because purchasers would not have road construction or logging costs—they would simply buy the wood from the log yard. Because the agencies may not be as efficient as a private enterprise, the agencies should consider contracting the log marketing business to a private business.

A secondary financial benefit would be the elimination of many opportunities for timber sale fraud and theft. Under harvest contracting, the scaling system would be eliminated and the contractor would not benefit from cutting trees designated to be left standing because of the fixed contract price and, in fact, might be penalized for not performing to contract specifications. That is why the bill contains a provision limiting the ability of the contractor who performs the contract from also selling the harvested wood.

Finally, this pilot project should benefit timber workers in several ways. First, salvage timber sales or thinning sales that were previously uneconomical to harvest would be offered, providing jobs for loggers and other resource experts. Second, timber companies would be purchasing wood after seeing its quality and knowing the exact board footage, rather than hypothesizing about the quantity of wood contained in a standing timber sale and not knowing how weather or timber markets might affect the ability to harvest or make a profit from the wood. Third, companies would not be subject to changes or delays in ability to harvest based on legal or political changes as they held long-term timber sale contracts; they would simply purchase wood.

While harvest contracting appears to offer many benefits from many different aspects, it remains untested on a large scale. This bill requires the Forest Service and BLM to establish pilot programs. This should provide guidance as to the feasibility, benefits, and drawbacks of the concept.

In addition, Senator MAX BAUCUS has introduced a bill, S. 1259, that also establishes a demonstration program to use stewardship contracting. The concepts contained in this bill were developed by a group of conservationists, forest product industry representatives, and community leaders. This should also offer guidance as to how to implement this pilot program.

FOREST TIMBER STAND STUDY TITLE IV

The Forest Service has initiated a similar study to that required in this bill. The Western Forest Health Initiative should be used as a foundation for the requirements of this bill. There is no need for the agencies to be duplicative, rather this bill's provisions should be supplemental to the work done in the WFHI.

COLLABORATIVE DECISIONMAKING

Early drafts of this bill included use of collaborative decisionmaking. The concept was dropped from the bill because it was too difficult to described in legislative language. However, this decisionmaking process was very effective when it was used to plan and develop timber salvage sales after the wildfires of 1994 on the Wenatchee National Forest. The process was developed by Steve Daniels and Gregg Walker, of Oregon State University, as a tool to support ecosystem-based management of forest.

Collaborative learning is a framework designed for natural resource management situations that have the following features: Multiple parties and issues, deeply held values and cultural difference, scientific and technical uncertainty, and legal and jurisdictional constraints. The key notions that define collaborative learning are: Redefining the task away from solving a problem to one of improving a situation; viewing the situation as a set of interrelated systems; defining improvement as desirable and feasible change;

recognizing that considerable learning about science, issues and value differences—will have to occur before implementable improvements are possible; and promoting working through the issues and perspectives of the situation.

Because of its success on the Wenatchee National Forest, I recommend the agencies consider use of collaborative decisionmaking procedures to increase valuable and productive participation by various interest parties.

By Mr. D'AMATO:

S.J. Res. 50. A joint resolution to disapprove the certification of the President under section 490(b) of the Foreign Assistance Act of 1961 regarding foreign assistance for Mexico during fiscal year 1996; to the Committee on Foreign Relations.

CERTIFICATION DISAPPROVAL LEGISLATION

Mr. D'AMATO. Mr. President, I rise today to introduce a joint resolution that disapproves of the administration's certification of Mexico. I am joined by my colleagues Senator HELMS, Senator MCCONNELL, and Senator PRESSLER in presenting this resolution and urge its immediate passage.

As a result of the amount of drugs that are found to have come into the United States through Mexico, we know that Mexico has failed to stem the international drug trade. If this administration does not want to recognize Mexico's failure, then it is up to Congress to do so. I will speak on this issue in more detail tomorrow. I encourage my colleagues to join us in this effort.

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

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

S.J. RES. 50

Resolved by the Senate and House of Representatives of the United States of America in Congress assembled, That pursuant to subsection (d) of section 490 of the Foreign Assistance Act of 1961 (22 U.S.C. 2291j), Congress disapproves the determination of the President with respect to Mexico for fiscal year 1996 that is contained in the certification (transmittal no.) submitted to Congress by the President under subsection (b) of that section on , 1996.

ADDITIONAL COSPONSORS

S. 953

At the request of Mr. DOLE, the names of the Senator from Kansas [Mrs. KASSEBAUM], the Senator from Michigan [Mr. ABRAHAM], and the Senator from Tennessee [Mr. FRIST] were added as cosponsors of S. 953, a bill to require the Secretary of the Treasury to mint coins in commemoration of black revolutionary war patriots.

At the request of Mr. CHAFEE, the names of the Senator from Wyoming [Mr. SIMPSON], the Senator from New Jersey [Mr. LAUTENBERG], the Senator from Virginia [Mr. ROBB], and the Senator from Mississippi [Mr. LOTT] were added as cosponsors of S. 953, supra.

At the request of Mr. BINGAMAN, his name was added as a cosponsor of S. 953, supra.

S. 1028

At the request of Mrs. KASSEBAUM, the name of the Senator from Alabama [Mr. SHELBY] was added as a cosponsor of S. 1028, a bill to provide increased access to health care benefits, to provide increased portability of health care benefits, to provide increased security of health care benefits, to increase the purchasing power of individuals and small employers, and for other purposes.

S. 1039

At the request of Mr. ABRAHAM, the names of the Senator from Kentucky [Mr. MCCONNELL] and the Senator from South Carolina [Mr. THURMOND] were added as cosponsors of S. 1039, a bill to require Congress to specify the source of authority under the United States Constitution for the enactment of laws, and for other purposes.

S. 1420

At the request of Mr. STEVENS, the names of the Senator from Illinois [Ms. MOSELEY-BRAUN] and the Senator from South Carolina [Mr. THURMOND] were added as cosponsors of S. 1420, a bill to amend the Marine Mammal Protection Act of 1972 to support International Dolphin Conservation Program in the eastern tropical Pacific Ocean, and for other purposes.

S. 1451

At the request of Mr. MCCAIN, the name of the Senator from South Dakota [Mr. PRESSLER] was added as a cosponsor of S. 1451, a bill to authorize an agreement between the Secretary of the Interior and a State providing for the continued operation by State employees of national parks in the State during any period in which the National Park Service is unable to maintain the normal level of park operations, and for other purposes.

S. 1483

At the request of Mr. KYL, the name of the Senator from Nevada [Mr. REID] was added as a cosponsor of S. 1483, a bill to control crime, and for other purposes.

S. 1506

At the request of Mr. ABRAHAM, the names of the Senator from Arizona [Mr. KYL] and the Senator from Missouri [Mr. BOND] were added as cosponsors of S. 1506, a bill to provide for a reduction in regulatory costs by maintaining Federal average fuel economy standards applicable to automobiles in effect at current levels until changed by law, and for other purposes.

S. 1548

At the request of Mrs. FEINSTEIN, the name of the Senator from North Carolina [Mr. HELMS] was added as a cosponsor of S. 1548, a bill to provide that applications by Mexican motor carriers of property for authority to provide service across the United States-Mexico international boundary line and by persons of Mexico who establish enterprises in the United States seeking to distribute international cargo in the United States shall not be approved until certain certifications are made to the Congress by the President and the Secretary of Transportation, and for other purposes.

S. 1553

At the request of Mr. MCCAIN, the names of the Senator from Louisiana [Mr. JOHNSTON], the Senator from Ohio [Mr. DEWINE], the Senator from Wyoming [Mr. THOMAS], the Senator from Alaska [Mr. STEVENS], the Senator from Missouri [Mr. ASHCROFT], the Senator from Louisiana [Mr. BREAUX], and the Senator from Minnesota [Mr. WELLSTONE] were added as cosponsors of S. 1553, a bill to provide that members of the Armed Forces performing services for the peacekeeping effort in the Republic of Bosnia and Herzegovina shall be entitled to certain tax benefits in the same manner as if such services were performed in a combat zone.

SENATE JOINT RESOLUTION 18

At the request of Mr. HOLLINGS, the name of the Senator from Mississippi [Mr. COCHRAN] was added as a cosponsor of Senate Joint Resolution 18, a joint resolution proposing an amendment to the Constitution relative to contributions and expenditures intended to affect elections for Federal, State, and local office.

SENATE JOINT RESOLUTION 49

At the request of Mr. KYL, the names of the Senator from North Carolina [Mr. HELMS] and the Senator from Michigan [Mr. ABRAHAM] were added as cosponsors of Senate Joint Resolution 49, a joint resolution proposing an amendment to the Constitution of the United States to require two-thirds majorities for bills increasing taxes.

SENATE RESOLUTION 133

At the request of Mr. HELMS, the name of the Senator from Arizona [Mr. KYL] was added as a cosponsor of Senate Resolution 133, a resolution expressing the sense of the Senate that the primary safeguard for the well-being and protection of children is the family, and that, because the United Nations Convention on the Rights of the Child could undermine the rights of the family, the President should not sign and transmit it to the Senate.

SENATE RESOLUTION 152

At the request of Mr. ABRAHAM, the names of the Senator from Kentucky [Mr. MCCONNELL] and the Senator from South Carolina [Mr. THURMOND] were added as cosponsors of Senate Resolution 152, a resolution to amend the Standing Rules of the Senate to require a clause in each bill and resolution to specify the constitutional authority of the Congress for enactment, and for other purposes.

SENATE RESOLUTION 224

At the request of Mr. D'AMATO, the names of the Senator from North Carolina [Mr. FAIRCLOTH], the Senator from Vermont [Mr. JEFFORDS], the Senator