105TH CONGRESS
1ST SESSION

S. 909

To encourage and facilitate the creation of secure public networks for communication, commerce, education, medicine, and government.

IN THE SENATE OF THE UNITED STATES

JUNE 16, 1997

Mr. MCCAIN (for himself, Mr. KERREY, and Mr. HOLLINGS) introduced the following bill; which was read twice and referred to the Committee on Commerce, Science, and Transportation

---

A BILL

To encourage and facilitate the creation of secure public networks for communication, commerce, education, medicine, and government.

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

SEC. 1. SHORT TITLE.

This Act may be cited as the "Secure Public Networks Act".

SEC. 2. DECLARATION OF POLICY.

It is the policy of the United States to encourage and facilitate the creation of secure public networks for com-

munication, commerce, education, research, medicine and government.

TITLE I—DOMESTIC USES OF ENCRYPTION

SEC. 101. LAWFUL USE OF ENCRYPTION.

Except as otherwise provided by this Act or otherwise provided by law, it shall be lawful for any person within any State to use any encryption, regardless of encryption algorithm selected, encryption key length chosen, or implementation technique or medium used.

SEC. 102. PROHIBITION ON MANDATORY THIRD PARTY ESCROW OF KEYS USED FOR ENCRYPTION OF CERTAIN COMMUNICATIONS.

Neither the Federal Government nor a State may require the escrow of an encryption key with a third party in the case of an encryption key used solely to encrypt communications between private persons within the United States.

SEC. 103. VOLUNTARY PRIVATE SECTOR PARTICIPATION IN KEY MANAGEMENT STRUCTURE.

The participation of the private persons in the key management infrastructure enabled by this Act is voluntary.

SEC. 104. UNLAWFUL USE OF ENCRYPTION.

Whoever knowingly encrypts data or communications in furtherance of the commission of a criminal offense for which the person may be prosecuted in a court of competent jurisdiction and may be sentenced to a term of imprisonment of more than one year shall, in addition to any penalties for the underlying criminal offense, be fined under title 18, United States Code, or imprisoned not more than five years, or both, for a first conviction or fined under title 18, United States Code, or imprisoned not more than ten years, or both, for a second or subsequent conviction. The mere use of encryption shall not constitute probable cause to believe that a crime is being or has been committed.

SEC. 105. PRIVACY PROTECTION.

(a) IN GENERAL.—It shall be unlawful for any person to intentionally—

(1) obtain or use recovery information without lawful authority for the purpose of decrypting data or communications;

(2) exceed lawful authority in decrypting data or communications;

(3) break the encryption code of another person without lawful authority for the purpose of violating the privacy, security or property rights of that person;

(4) intercept on a public communications network without lawful authority the intellectual property of another person for the purpose of violating the intellectual property rights of that person;

(5) impersonate another person for the purpose of obtaining recovery information of that person without lawful authority;

(6) issue a key to another person in furtherance of a crime;

(7) disclose recovery information in violation of a provision of this Act; or

(8) publicly disclose without lawful authority the plaintext of information that was decrypted using recovery information obtained with or without lawful authority.

(b) CRIMINAL PENALTY.—Any person who violates this section shall be fined under title 18, United States Code, or imprisoned not more than five years, or both.

SEC. 106. ACCESS TO ENCRYPTED MESSAGES BY GOVERNMENT ENTITIES.

(1) EFFECT ON EXISTING AUTHORITIES.—Nothing in this section authorizes a government entity to obtain recovery information from any key recovery agent unless the government entity has lawful authority to obtain com-

munications or electronically stored information apart from this Act.

(2) LAWFUL PURPOSES.—A key recovery agent, whether or not registered by the Secretary under this Act, shall disclose recovery information:

(a) To a government entity if that entity is authorized to use the recovery information to determine the plaintext of information it has obtained or is obtaining pursuant to a duly-authorized warrant or court order, a subpoena authorized by Federal or State statute or rule, a certification issued by the Attorney General under the Foreign Intelligence Surveillance Act, or other lawful authority; or

(b) To a government entity to permit that entity to comply with a request from a foreign government that the entity is authorized to execute under United States law.

(3) PROCEDURES.—A key recovery agent, whether or not registered by the Secretary under this Act, shall disclose recovery information to a Federal or State government entity, to permit it to achieve the lawful purposes specified in subsection (2) of this section upon the receipt of a subpoena described in subsection (4) which is based upon a duly authorized warrant or court order authorizing interception of wire communications or electronic commu-

nications authorized under chapter 119 or title 18, United States code, or applicable State statute, or authorizing access to stored wire and electronic communications and transactional records under chapter 121 of title 18, United States Code, or applicable State statute; a subpoena authorized by or based on authority established by Federal or State law, statute, precedent or rule; a warrant or court order or certification issued by the Attorney General authorized under the Foreign Intelligence Surveillance Act, 50 United State Code 1801 et seq. or other lawful authority, and directing such key recovery agent to provide assistance.

(4) SUBPOENA.—The Attorney General shall by rule prescribe the form of a uniform subpoena and identify the necessary endorsements for such a subpoena to ensure the lawful disclosure of key recovery information to a Federal or State government entity by a Key Recovery Agent authorized under subsection (2) of this section.

(5) AUDITS.—The Attorney General shall establish periodic audits of subpoenas issued under this section to ensure that subpoenas issued are pursuant to lawful authority. In the event an audit finds a subpoena issued without lawful authority, the Attorney General shall ensure that necessary disciplinary, investigatory, and prosecutorial steps are taken.

SEC. 107. CIVIL RECOVERY.

(a) IN GENERAL.—Except as otherwise provided in this Act, any person described in subsection (b) may in a civil action recover from the United States Government the actual damages suffered by the person as result of a violation described in that subsection, a reasonable attorney's fee, and other litigation costs reasonably incurred.

(b) COVERED PERSONS.—Subsection (a) applies to any person—

(1) whose recovery information is knowingly obtained without lawful authority by an agent of the United States Government from a key recovery agent or certificate authority registered under this Act;

(2) whose recovery information is obtained by an agent of the United States Government with lawful authority from a key recovery agent or certificate authority registered under this Act and is knowingly used or disclosed without lawful authority; or

(3) whose recovery information is obtained by an agent of the United States Government with lawful authority from a key recovery agent or certificate authority registered under this Act and is used to publicly disclose decrypted information without lawful authority.

(c) LIMITATION.—A civil action under this section shall be commenced not later than two years after the date on which the claimant first discovers the violation.

SEC. 108. USE AND HANDLING OF DECRYPTED INFORMATION.

(a) AUTHORIZED USE OF DECRYPTED INFORMATION.—A government entity to which recovery information is released in accordance with this Act may use the plaintext information obtained with the recovery information only for lawful purposes.

(b) HANDLING OF DECRYPTED INFORMATION.—Upon completion of the use of plaintext information obtained with recovery information released under this Act, the government entity concerned shall handle and protect the privacy of the plaintext information in a manner consistent with applicable Federal or State statute, law or rule.

SEC. 109. USE AND DESTRUCTION OR RETURN OF RECOVERY INFORMATION.

(a) AUTHORIZED USE OF RECOVERY INFORMATION.—

(1) IN GENERAL.—A government entity to which recovery information is released under this Act may use the recovery information only for lawful purposes.

(2) LIMITATION.—A government entity may not use recovery information obtained under this Act to determine the plaintext of any wire communication or electronic communication or of any stored electronic information unless it has lawful authority to determine the plaintext under provisions of law other than this Act.

(b) RETURN OR DESTRUCTION OF INFORMATION.—Upon completion of the use of recovery information obtained under this Act, the government entity concerned shall unless otherwise required by law destroy the information or return the information to the key recovery agent and shall make a record documenting such destruction or return.

(c) NOTICE.—When a government entity destroys a key pursuant to this section, the government entity shall notify the key recovery agent of such destruction.

SEC. 110. DISCLOSURE OR RELEASE OF RECOVERY INFORMATION.

Except as otherwise authorized by this Act, a key recovery agent or other person may not disclose to any person the facts or circumstances of any release of recovery information pursuant to section 106, or of any requests therefor, unless under an order by a Federal court of competent jurisdiction.

SEC. 111. NOTIFICATION TO RECIPIENTS OF RECOVERY INFORMATION.

A key recovery agent or certificate authority, whether or not registered under this Act, who discloses recovery information shall—

(1) notify the recipient that recovery information is being disclosed; and

(2) specify which part of the information disclosed is recovery information.

TITLE II—GOVERNMENT PROCUREMENT

SEC. 201. POLICY.

It is the policy of the United States Government to facilitate the creation of secure networks that permit the public to interact with the government through networks which protect privacy, the integrity of information, rights in intellectual property, and the personal security of network users.

SEC. 202. FEDERAL PURCHASES OF ENCRYPTION PRODUCTS.

Any encryption product purchased or otherwise procured by the United States Government for use in secure government networks shall be based on a qualified system of key recovery.

SEC. 203. ENCRYPTION PRODUCT PURCHASED WITH FEDERAL FUNDS.

Any encryption product purchased directly with Federal funds for use in secure public networks shall be based on a qualified system of key recovery.

SEC. 204. UNITED STATES GOVERNMENT NETWORKS.

Any communications network established by the United States Government after the date of enactment of this Act which uses encryption products as part of the network shall use encryption products based on a qualified system of key recovery.

SEC. 205. NETWORKS ESTABLISHED WITH FEDERAL FUNDS.

Any encrypted communications network established after the date of enactment of this Act with the use of Federal funds shall use encryption products based on a qualified system of key recovery.

SEC. 206. PRODUCT LABELS.

An encryption product may be labeled to inform users that the product is authorized for sale to or for use in transactions and communications with the United States Government under this title.

SEC. 207. NO PRIVATE MANDATE.

The United States Government may not mandate the use of encryption standards for the private sector other than for use with computer systems, networks or other

systems of the United States Government, or systems or networks created using Federal funds.

SEC. 208. TRANSITION RULES.

The Secretary may though rule provide for the orderly implementation of this section and the effective use of secure public networks.

SEC. 209. INTEROPERABILITY.

In establishing the criteria for a qualified system of key recovery, the Secretary shall consider providing for the interoperability of key recovery products procured under this section with non-key recovery products to ensure that citizens have secure network access to their government.

TITLE III—EXPORT OF ENCRYPTION

SEC. 301. THE DEPARTMENT OF COMMERCE.

The Secretary of Commerce in consultation with other relevant executive branch agencies shall have jurisdiction over the export of commercial encryption products. The Secretary shall have the sole duty to issue export licenses on commercial encryption products.

SEC. 302. LICENSE EXCEPTION NON-KEY RECOVERY.

Exports of encryption products up to and including 56 bit DES or equivalent strength shall be exportable under a license exception, following a one time receive, provided the encryption product being exported—

(1) is otherwise qualified for export;

(2) is otherwise legal;

(3) does not violate U.S. law;

(4) does not violate the intellectual property rights of another; and

(a) the recipient individual is otherwise qualified to review such encryption product; and

(b) the country to which the encryption product is to be exported is otherwise qualified to receive the encryption product.

The Secretary shall complete a license exception review under this section within ten working days of a properly filed license exception request.

SEC. 303. PRESIDENTIAL ORDER.

The President may be executive order increase the encryption strength for encryption products which may be exported under section 302 of this Act. The encryption strength for encryption products which may be exported under section 302 of this Act shall be reviewed by the President on an annual basis. Consistent with other provisions of this Title and Section 901 of this Act, the President shall take such action as necessary to increase the encryption strength for encryption products which may be exported if similar products are determined by the President to be widely available for export from other Nations.

SEC. 304. LICENSE EXCEPTION FOR KEY RECOVERY.

Encryption products may be exported under a license exception, following a one time review without regard to the encryption algorithm selected or encryption key length chosen when such encryption product is based on a qualified system of key recovery, provided, the encryption product being exported—

(1) is otherwise qualified for export;

(2) is otherwise legal;

(3) does not violate U.S. law;

(4) does not violate the intellectual property right of another; and

(a) the recipient individual is otherwise qualified to receive such product; and

(b) the country to which the encryption product is to be exported is otherwise qualified to receive the encryption product.

The Secretary shall describe the elements of a qualified system of key recovery and the procedures for establishing compliance with those elements. The Secretary shall complete a license exception review under this section within ten working days of a properly filed license exception request.

SEC. 305. EXPEDITED REVIEW FOR CERTAIN INSTITUTIONS.

The Secretary in consultation with other relevant executive branch agencies shall establish a procedure for ex-

pedited review of export license applications involving encryption products for use by qualified Banks, Financial Institutions and Health Care Providers, subsidiaries of U.S. Owned and controlled companies or other users authorized by the Secretary.

SEC. 306. PROHIBITED EXPORTS.

The export of any encryption product shall be prohibited when the Secretary in consultation with other agencies finds evidence that the encryption product to be exported would be used in acts against the national security, the public safety, transportation systems, communications networks, financial institutions or other essential systems of interstate commerce; diverted to a military, terrorist or criminal use; or re-exported without authorization. The Secretary's decision on the grounds for a prohibition under his section shall not be subject to judicial review.

SEC. 307. LICENSE REVIEW.

In evaluating applications for export licenses for encryption products not based on a qualified key recovery system, in strengths above the level described in Section 302, the following factors shall be among those considered by the Secretary:

(1) whether an encryption product is generally available and is designed for installation without alteration by purchaser;

(2) whether the encryption product is generally available in the country to which the encryption product would be exported;

(3) whether encryption products offering comparable security and level of encryption is available in the country to which the encryption product would be exported; or

(4) whether the encryption product will be imminently available in the country to which the product would be exported.

The Secretary shall complete a license review under this section within thirty working days of a properly filed license request. The Secretary's decision on the grounds for the grant or denial of license shall not be subject to judicial review.

SEC. 308. CRIMINAL PENALTIES.

Any person who exports an encryption product in violation of this Title shall be fined under Title 18, United States Code or imprisoned for not more than five years.

TITLE IV—VOLUNTARY REGISTRATION SYSTEM

SEC. 401. VOLUNTARY USE OF CERTIFICATE AUTHORITIES AND KEY RECOVERY AGENTS.

Except as provided in Title II of this Act, nothing in this Act may be construed to require a person, in com-

munications between private persons within the United States, to—

(1) use an encryption product with a key recovery feature;

(2) use a public key issued by a certificate authority registered under this Act; or

(3) entrust key recovery information with a key recovery agent registered under this Act.

SEC. 402. REGISTRATION OF CERTIFICATE AUTHORITIES.

(a) AUTHORITY TO REGISTER.—The Secretary or the Secretary's designee may register any private person, entity, government entity, or foreign government agency to act as a certificate authority if the Secretary determines that the person, entity or agency meets such standards relating to security in and performance of the activities of a certificate authority registered under this Act.

(b) AUTHORIZED ACTIVITIES OF REGISTERED CERTIFICATE—AUTHORITIES.—

(1) A certificate authority registered under this section may issue public key certificates which may be used to verify the identity of a person engaged in encrypted communications for such purposes as authentication, integrity, nonrepudiation, digital signature, and other similar purposes.

(2) A certificate authority registered under this section may issue public key certificates which may be used for encryption.

(3) The Secretary shall not, as a condition of registration under this Act, require any certificate authority to store with a third party information used solely for the purposes in subparagraph (b)(1) of this section.

(c) CONDITION MODIFICATION AND REVOCATION OF REGISTRATION.—The Secretary may condition, modify or revoke the registration of a certificate authority under this section if the Secretary determines that the certificate authority has violated any provision of this Act, or any regulations thereunder, or for any other reason specified in such regulations.

(d) REGULATIONS.—

(1) REQUIREMENT.—The Secretary in consultation with other relevant executive branch agencies shall prescribe regulations relating to certificate authorities registered under this section. The regulations shall be consistent with the purposes of this Act.

(2) ELEMENTS.—The regulations prescribed under this subsection shall—

(A) establish requirements relating to the practices of certificate authorities, including the basis for the modification or revocation of registration under subsection (c);

(B) specify reasonable requirements for public key certificates issued by certificate authorities which requirements shall meet generally accepted standards for such certificates;

(C) specify reasonable requirements for record keeping by certificate authorities;

(D) specify reasonable requirements for the content, form, and sources of information in disclosure records of certificate authorities, including the updating and timeliness of such information, and for other practices and policies relating to such disclosure records; and

(E) otherwise give effect to and implement the provisions of this Act relating to certificate authorities.

SEC. 403. REGISTRATION OF KEY RECOVERY AGENTS.

(a) AUTHORITY TO REGISTER.—The Secretary or the Secretary's designee may register a private person, entity, or government entity to act as a key recovery agent if the Secretary determines that the person or entity pos-

sesses the capability, competency, trustworthiness, and resources to

(1) safeguard sensitive information;

(2) carry out the responsibilities set forth in subsection (b); and

(3) comply with such regulations relating to the practices of key recovery agents as the Secretary shall prescribe.

(b) RESPONSIBILTIEIS OF KEY RECOVERY AGENTS.—A key recovery agent registered under subsection (a) shall, consistent with any regulations prescribed under subsection (a), establish procedures and take other appropriate steps to—

(1) ensure the confidentiality, integrity, availability, and timely release of recovery information held by the key recovery agent;

(2) protect the confidentiality of the identity of the person or persons for whom the key recovery agent holds recovery information;

(3) protect the confidentiality of lawful requests for recovery information, including the identity of the individual or government entity requesting recovery information and information concerning access to and use of recovery information by the individual or entity; and

(4) carry to the responsibilities of key recovery agents set forth in this Act and the regulations thereunder.

(c) CONDITION, MODIFICATION OR REVOCATION OF REGISTRATION.—The Secretary may condition, modify or revoke the registration of a key recovery agent under this section if the Secretary determines that the key recovery agent has violated any provision of this Act, or any regulations thereunder, or for any other reason specified in such regulations.

(d) REGULATIONS.—The Secretary in consultation with other relevant executive branch agencies shall prescribe regulations relating to key recovery agents registered under this section. The regulations shall be consistent with the purposes of this Act.

SEC. 404. DUAL REGISTRATION AS KEY RECOVERY AGENT AND CERTIFICATE AUTHORITY.

Nothing in this Act shall be construed to prohibit the registration as a certificate authority under section 402 of a person or entity registered as a key recovery agent under section 403.

SEC. 405. PUBLIC KEY CERTIFICATES FOR ENCRYPTION KEYS.

The Secretary or a Certificate Authority for Public Keys registered under this Act may issue to a person a

public key certificate that certificates a public key that can be used for encryption only if the person:

(1) stores with a Key Recovery Agent registered under this Act sufficient information, as specified by the Secretary in regulations, to allow timely lawful recovery of the plaintext of that person's encrypted data and communications; or

(2) makes other arrangements, approved by the Secretary pursuant to regulations promulated in concurrence with the Attorney General, that assure that lawful recovery of the plaintext of encrypted data and communications can be accomplished in a timely fashion and, unless authorized under Section 110 of this Act, without disclosing that data or communications are being recovered pursuant to a government request.

SEC. 406. DISCLOSURE OR RECOVERY INFORMATION.

A key recovery agent, whether or not registered under this Act, may not disclose recovery information stored with the key recovery agent by a person unless the disclosure is—

(1) to the person, or an authorized agent thereof;

(2) with the consent of the person, including pursuant to a contract entered into with the person;

(3) pursuant to a court order upon a showing of compelling need for the information that cannot be accommodated by any other means if—

(A) the person who supplied the information is given reasonable notice, by the person seeking the disclosure, of the court proceeding relevant to the issuance of the court order; and

(B) the person who supplied the information is afforded the opportunity to appear in the court proceeding and contest the claim of the person seeking the disclosure;

(4) pursuant to a determination by a court of competent jurisdiction that another person is lawfully entitled to hold such recovery information, including determinations arising from legal proceedings associated with the incapacity, death, or dissolution of any person; or

(5) otherwise permitted by a provision of this Act or otherwise permitted by law.

SEC. 407. CRIMINAL ACTS.

(a) IN GENERAL.—It shall be unlawful for—

(1) a certificate authority registered under this Act, or an officer, employee, or agent thereof, to intentionally issue a public key certificate in violation of this Act;

(2) any person to intentionally issue what purports to be a public key certificate issued by a certificate authority registered under this Act when such person is not a certificate authority registered under this Act;

(3) any person to fail to revoke what purports to be a public key certificate issued by a certificate authority registered under this Act when such person knows that the issuing person is not such a certificate authority and have the power to revoke a public key certificate;

(4) any person to intentionally issue a public key certificate to a person who does not meet the requirements of this Act or the regulations prescribed thereunder; or

(5) any person to intentionally apply for or obtain a public key certificate under this Act knowing that the person to be identified in the public key certificate does not meet the requirements of this Act or the regulations thereunder.

(b) CRIMINAL PENALTY.—Any person who violates this section shall be fined under title 18, United States Code, or imprisoned not more than five years, or both.

TITLE V-LIABILITY LIMITATIONS

SEC. 501. NO CAUSE OF ACTION FOR COMPLYING WITH GOVERNMENT REQUESTS.

No civil or criminal liability under this Act, or under any other provision of law, shall attach to any key recovery agent, or any officer, employee, or agent thereof, or any other persons specified by the Secretary in regulations, for disclosing recovery information or providing other assistance to a government entity in accordance with sections 106 and 406 of this Act.

SEC. 502. COMPLIANCE DEFENSE.

Compliance with the provisions of this Act and the regulations thereunder is a complete defense for certificate authorities and key recovery agents registered under this Act to any noncontractual civil action for damages based upon activities regulated by this Act.

SEC. 503. REASONABLE CARE DEFENSE.

The use by any person of a certificate authority or key recovery agent registered under this Act shall be treated as evidence of reasonable care or due diligence in any judicial or administrative proceeding where the reasonableness of the selection of the authority or agent, as the case may be, or of encryption products, is a material issue.

SEC. 504. GOOD FAITH DEFENSE.

A good faith reliance on legal authority requiring or authorizing access to recovery information under this Act, or any regulations thereunder, is a complete defense to any criminal action brought under this Act or any civil action.

SEC. 505. LIMITATION ON FEDERAL GOVERNMENT LIABILITY.

Except as otherwise provided in this Act, the United States shall not be liable for any loss incurred by any individual or entity resulting from any violation of this Act or the performance or nonperformance of any duties under any regulation or procedure established by or under this Act, nor resulting from any action by any person who is not an official or employee of the United States.

SEC. 506. CIVIL ACTION

Civil action may be brought against a key recovery agent, a certificate authority or other person who violates or acts in a manner which is inconsistent with this Act.

TITLE VI—INTERNATIONAL AGREEMENTS

The President shall conduct negotiations with other countries for the purpose of mutual recognition of key recovery agents and certificate authorities; and to safeguard privacy and prevent commercial espionage. The President shall consider a country's refusal to negotiate such mutual

recognition agreements when considering the participation of the United States in any cooperation or assistance program with that country. The President shall report to the Congress if negotiations are not complete by the end of 1999.

TITLE VII—GENERAL AUTHORITY AND CIVIL PENALTIES

SEC. 701. GENERAL AUTHORITY AND CIVIL REMEDIES.

(a) AUTHORITIES TO SECURE INFORMATION.—To the extent necessary or appropriate to the enforcement of this Act or any regulation thereunder, the Secretary may make investigations, obtain information, take sworn testimony, and require reports or the keeping of records by and make inspection of the books, records, and other writings, premises or property of any person.

(b) INVESTIGATIONS.—

(1) APPLICABLE AUTHORITIES.—In conducting investigations under subsection (a) the Secretary may, to the extent necessary or appropriate to the enforcement of this Act and subject to such requirements as the Attorney General shall prescribe, exercise such authorities as are conferred upon the Secretary by other laws of the United States.

(2) ADDITIONAL AUTHORITY.—In conducting such investigations, the Secretary may administer

oaths or affirmations and may by subpoena require any person to appear and testify or to appear and produce books, records, and other writings, or both.

(3) WITNESSES AND DOCUMENTS.—

(A) IN GENERAL.—The attendance of witnesses and the production of documents provided for in this subsection may be required in any State at any designated place.

(B) WITNESS FEES.—Witnesses summoned shall be paid the same fees and mileage that are paid to witnesses in the courts of the United States.

(4) ORDERS TO APPEAR.—In the case of contumacy by, or refusal to obey a subpoena issued to any person pursuant to this subsection, the district court of the United States for the district in which such person is found, resides, or transacts business, upon application by the United States and after notice to such person, shall have jurisdiction to issue an order requiring such person to appear and give testimony before the Secretary or to appear and produce documents before the Secretary, or both, and any failure to obey such order of the court may be punished by such court as a contempt thereof.

SEC. 702. CIVIL PENALTIES.

(a) AUTHORITY TO IMPOSE CIVIL PENALTIES.—

(1) IN GENERAL.—The Secretary may, after notice and an opportunity for an agency hearing on the record in accordance with sections 554 through 557 of title 5, United States Code, impose a civil penalty of not more than $100,000 for each violation of this Act or any regulation thereunder either in addition to or in lieu of any other liability or penalty which may be imposed for such violation.

(2) CONSIDERATION REGARDING AMOUNT.—In determining the amount of the penalty, the Secretary shall consider the risk of harm to law enforcement, public safety, and national security, the risk of harm to affected persons, the gross receipts of the charged party, and the willfulness of the violation.

(3) LIMITATION.—Any proceeding in which a civil penalty is sought under this subsection may not be initiated more than 5 years after the date of the violation.

(4) JUDICIAL REVIEW.—The imposition of a civil penalty under paragraph (1) shall be subject to judicial review in accordance with sections 701 through 706 of title 5, United States Code.

(b) RECOVERY.—

(1) IN GENERAL.—A civil penalty under this section, plus interest at the currently prevailing rates from the date of the final order, may be recovered in an action brought by the Attorney General on behalf of the United States in the appropriate district court of the United States. In such action, the validity and appropriateness of the final order imposing the civil penalty shall not be subject to review.

(2) LIMITATION.—No action under this subsection may be commenced more than 5 years after the order imposing the civil penalty concerned becomes final.

SEC. 703. INJUNCTIONS.

The Attorney General may bring an action to enjoin any person from committing any violation of any provision of this Act or any regulation thereunder.

SEC. 704. JURISDICTION.

The district courts of the United States shall have original jurisdiction over any action brought by the Attorney General under this title.

TITLE VIII—RESEARCH AND MONITORING

SEC. 801. INFORMATION SECURITY BOARD.

(a) REQUIREMENT TO ESTABLISH.—The President shall establish an advisory board to be known as the Information Security Board (in this section referred to as the "Board").

(b) MEMBERSHIP.—The Board shall be composed of—

(1) such number of members as the President shall appoint from among the officers or employees of the Federal Government involved in the formation of United States policy regarding secure public networks, including United States policy on exports of products with information security features; and

(2) a number of members equal to the number of members under paragraph (1) appointed by the President from among individuals in the private sector having an expertise in information technology or in law or policy relating to such technology.

(c) MEETINGS.—The Board shall meet not less often than once each year.

(d) DUTIES.—The Board shall review available information and make recommendations to the President and Congress on appropriate policies to ensure—

(1) the security of networks;

(2) the protection of intellectual property rights in information and products accessible through computer networks;

(3) the promotion of exports of software produced in the United States;

(4) the national security, effective law enforcement, and public safety interests of the United States related to communications networks; and

(5) the protection of the interests of Americans in the privacy of data and communications.

SEC. 802. COORDINATION OF ACTIVITIES ON SECURE PUBLIC NETWORKS.

In order to meet the purposes of this Act, the President shall—

(1) ensure a high level of cooperation and coordination between the departments and agencies of the Federal Government in the formation and discharge of United States policy regarding secure public networks; and

(2) encourage cooperation and coordination between the Federal Government and State and local governments in the formation and discharge of such policy.

SEC. 803. NETWORK RESEARCH.

It shall be a priority of the Federal Government to encourage research to facilitate the creation of secure public networks which satisfy privacy concerns, national security interests, effective law enforcement requirements, and public safety needs.

SEC. 804. ANNUAL REPORT.

(a) REQUIREMENT.—The National Telecommunications and Information Administration shall, in consultation with other Federal departments and agencies, submit to Congress and the President each year a report on developments in the creation of secure public networks in the United States.

(b) ELEMENTS.—The report shall discuss developments in encryption, authentication, identification, and security on communications networks during the year preceding the submittal of the report and may include recommendations on improvements in United States policy to such matters.

SEC. 805. NATIONAL PERFORMANCE REVIEW.

The National Performance Review shall evaluate the progress of federal efforts to migrate government services and operations to secure public networks.

SEC. 806. EDUCATION NETWORKS.

The Department of Education, in cooperation with the National Telecommunications and Information Ad-

ministration and the Federal Communications Commission and the Joint Board established by the Federal Communications Commission and State Departments of Education shall evaluate technical, educational, legal and regulatory standards for distance learning via secure public networks.

TITLE IX—WAIVER AUTHORITY

SEC. 901. WAIVER AUTHORITY.

(a) AUTHORITY TO WAIVE.—The President may by executive order waive provisions of this Act, or the applicability of any such provision to a person or entity, if the President determines that the waiver is in the interests of national security, or domestic safety and security.

(b) REPORT.—Not later than 15 days after each exercise of authority provided in subsection (a), the President shall submit to Congress a report on the exercise of the authority, including the determination providing the basis of the exercise of the authority. The report shall explain the grounds of the President's action with specificity and be submitted in unclassified and classified form.

TITLE X—MISCELLANEOUS PROVISIONS

SEC. 1001. REGULATION AND FEES.

(a) REGULATIONS.—The Secretary shall, in consultation with the Secretary of State, the Secretary of Defense,

and the Attorney General and after notice to the public and opportunity for comment, prescribe any regulations necessary to carry out this Act.

(b) FEES.—The Secretary may provide in the regulations prescribed under subsection (a) for the imposition and collection of such fees as the Secretary considers appropriate for purposes of this Act.

SEC. 1002. INTERPRETATION.

Nothing contained in this Title shall be deemed to:

(1) pre-empt or otherwise affect the application of the Arms Export Control Act (22 U.S.C. 2751 et seq.), the Export Administration Act of 1979, as amended (50 U.S.C. app. 2401–2420), and the International Emergency Economic Powers Act (50 U.S.C. 1701–1706), or regulations promulgated thereunder;

(2) affect intelligence activities outside the United States;

(3) or weaken any intellectual property protection.

SEC. 1003. SEVERABILITY.

If any provision of this Act, or the application thereof, to any person or circumstances is held invalid, the remainder of this Act, and the application thereof, to other persons or circumstances shall not be affected thereby.

SEC. 1004. AUTHORIZATION OF APPROPRIATIONS.

There are hereby authorized to be appropriated to the Secretary of Commerce for fiscal years 1998, 1999, 2000, 2001, and 2002 such sums as may be necessary to carry out responsibilities under this Act.

SEC. 1005. DEFINITIONS.

For purposes of this Act:

(1) CERTIFICATE AUTHORITY.—The term "certificate authority" means a person trusted by one or more persons to create and assign public key certificates.

(2) DECRYPTION.—The term "decryption" means the electronic retransformation of data (including communications) that has been encrypted into the data's original form. To "decrypt" is to perform decryption.

(3) ELECTRONIC COMMUNICATION.—The term "electronic communication" has the meaning given such term in section 2510(12) of title 18, United States Code.

(4) ELECTRONIC INFORMATION.—The term "electronic information" includes voice communications, texts, messages, recordings, images, or documents in any electronic, electromagnetic, photoelectronic, photooptical, or digitally encoded computer-readable form.

(5) ELECTRONIC STORAGE.—The term "electronic storage" has the meaning given that term in section 2510(17) of title 18, United States Code.

(6) ENCRYPTION.—The term "encryption" means the electronic transformation of data (including communications) in order to hide its information content. To "encrypt" is to perform encryption.

(7) ENCRYPTION PRODUCT.—The term "encryption product" includes any product, software, or technology used to encrypt and decrypt electronic messages and any product software or technology with encryption capabilities.

(8) KEY.—The term "key" means a parameter, or a component thereof, used with an algorithm to validate, authenticate, encrypt, or decrypt data or communications.

(9) KEY RECOVERY AGENT.—

(A) IN GENERAL.—The term "key recovery agent" means a person trusted by one or more persons to hold and maintain sufficient information to allow access to the data or communications of the person or persons for whom that information is held, and who holds and maintains that information as a business or

governmental practice, whether or not for profit.

(B) INCLUSION.—The term "key recovery agent" includes any person who holds the person's own recovery information.

(10) PERSON.—The term "person" means any individual, corporation, company, association, firm, partnership, society, or joint stock company.

(11) PLAINTEXT.—The term "plaintext" refers to data (including communications) that has not been encrypted or, if encrypted, has been decrypted.

(12) PUBLIC KEY.—The term "public key" means, for cryptographic systems that use different keys for encryption and decryption, the key that is intended to be publicly known.

(13) PUBLIC KEY CERTIFICATE.—The term "public key certificate" means information about a public key and its user, particularly including information that identifies that public key with its user, which has been digitally signed by the person issuing the public key certificate, using a private key of the issuer.

(14) QUALIFIED SYSTEM OF KEY RECOVERY.—The term "qualified system of key recovery" means a method of encryption which meets the criteria es-

tablished by the Secretary and provides for the recovery of keys and may include the use of split keys, multiple key systems or other system approved by the Secretary, or a system which otherwise provides for the timely and unlawful access to plaintext, and meets the criteria established by the Secretary.

(15) RECOVERY INFORMATION.—The term "recovery information" means a key or other information provided to a key recovery agent by a person that can be used to decrypt the data or communications of the person.

(16) SECRETARY.—The term "Secretary" means the Secretary of Commerce.

(17) STATE.—The term "State" has the meaning given the term in section 2510(3) of title 18, United States Code.

(18) STORED ELECTRONIC INFORMATION.—The term "stored electronic information" means any wire communication or electronic communication that is in electronic storage.

(19) WIRE COMMUNICATION.—The term "wire communication" has the meaning given that term in section 2510(1) of title 18, United States Code.

O

Document No. 152