106TH CONGRESS
1st Session
HOUSE OF REPRESENTATIVES
REPT. 106–117
Part 5

ENCRYPTION FOR THE NATIONAL INTEREST ACT

JULY 23, 1999.—Committed to the Committee of the Whole House on the State of the Union and ordered to be printed

---

Mr. GOSS, from the Permanent Select Committee on Intelligence, submitted the following

R E P O R T

[To accompany H.R. 850]

[Including cost estimate of the Congressional Budget Office]

The Permanent Select Committee on Intelligence, to whom was referred the bill (H.R. 850) to amend title 18, United States Code, to affirm the rights of United States persons to use and sell encryption and to relax export controls on encryption, having considered the same, report favorably thereon with an amendment and recommend that the bill as amended do pass.

The amendment is as follows:

Strike out all after the enacting clause and insert in lieu thereof the following:

SECTION 1. SHORT TITLE; TABLE OF CONTENTS.

(a) SHORT TITLE.—This Act may be cited as the "Encryption for the National Interest Act".

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

SEC. 2. STATEMENT OF POLICY.

It is the policy of the United States to protect public computer networks through the use of strong encryption technology, to promote the export of encryption products developed and manufactured in the United States, and to preserve public safety and national security.

SEC. 3. CONGRESSIONAL FINDINGS.

The Congress finds the following:

(1) Information security technology, encryption, is—

(A) fundamental to secure the flow of intelligence information to national policy makers;

(B) critical to the President and national command authority of the United States;

(C) necessary to the Secretary of State for the development and execution of the foreign policy of the United States;

(D) essential to the Secretary of Defense's responsibilities to ensure the effectiveness of the Armed Forces of the United States;

(E) invaluable to the protection of the citizens of the United States from fraud, theft, drug trafficking, child pornography; kidnapping, and money laundering; and

(F) basic to the protection of the nation's critical infrastructures, including electrical grids, banking and financial systems, telecommunications, water supplies, and transportation.

(2) The goal of any encryption legislation should be to enhance and promote the global market strength of United States encryption manufacturers, while guaranteeing that national security and public safety obligations of the Government can still be accomplished.

(3) It is essential to the national security interests of the United States that United States encryption products dominate the global market.

(4) Widespread use of unregulated encryption products poses a significant threat to the national security interests of the United States.

(5) Leaving the national security and public safety responsibilities of the Government to the marketplace alone is not consistent with the obligations of the Government to protect the public safety and to defend the Nation.

(6) In order for the United States position in the global market to benefit the national security interests of the United States, it is imperative that the export of encryption products be subject to a dynamic and constructive export control regime.

(7) Export of commercial items are best managed through a regulatory structure which has flexibility to address constantly changing market conditions.

(8) Managing sensitive dual-use technologies, such as encryption products, is challenging in any regulatory environment due to the difficulty in balancing competing interests in national security, public safety, privacy, fair competition within the industry, and the dynamic nature of the technology.

(9) There is a widespread perception that the executive branch has not adequately balanced the equal and competing interests of national security, public safety, privacy, and industry.

(10) There is a perception that the current encryption export control policy has done more to disadvantage United States business interests than to promote and protect national security and public safety interests.

(11) A balance can and must be achieved between industry interests, national security, law enforcement requirements, and privacy needs.

(12) A court order process should be required for access to plaintext, where and when available, and criminal and civil penalties should be imposed for misuse of decryption information.

(13) Timely access to plaintext capability is—

(A) necessary to thwarting potential terrorist activities;

(B) extremely useful in the collection of foreign intelligence;

(C) indispensable to force protection requirements;

(D) critical to the investigation and prosecution of criminals; and

(E) both technically and economically possible.

(14) The United States Government should encourage the development of those products that would provide a capability allowing law enforcement (Federal, State, and local), with a court order only, to gain timely access to the plaintext of either stored data or data in transit.

(15) Unless law enforcement has the benefit of such market encouragement, drug traffickers, spies, child pornographers, pedophiles, kidnappers, terrorists, mobsters, weapons proliferators, fraud schemers, and other criminals will be able to use encryption software to protect their criminal activity and hinder the criminal justice system.

(16) An effective regulatory approach to manage the proliferation of encryption products which have dual-use capabilities must be maintained and greater confidence in the ability of the executive branch to preserve and promote the competitive advantage of the United States encryption industry in the global market must be provided.

TITLE I—DOMESTIC USES OF ENCRYPTION

SEC. 101. DEFINITIONS.

For purposes of this Act:

(1) ATTORNEY FOR THE GOVERNMENT.—The term "attorney for the Government" has the meaning given such term in Rule 54(c) of the Federal Rules of Criminal Procedure, and also includes any duly authorized attorney of a State who is authorized to prosecute criminal offenses within such State.

(2) AUTHORIZED PARTY.—The term "authorized party" means any person with the legal authority to obtain decryption information or plaintext of encrypted data, including communications.

(3) COMMUNICATIONS.—The term "communications" means any wire communications or electronic communications as those terms are defined in paragraphs (1) and (12) of section 2510 of title 18, United States Code.

(4) COURT OF COMPETENT JURISDICTION.—The term "court of competent jurisdiction" means any court of the United States organized under Article III of the Constitution of the United States, the court organized under the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.), or a court of general criminal jurisdiction of a State authorized pursuant to the laws of such State to enter orders authorizing searches and seizures.

(5) DATA NETWORK SERVICE PROVIDER.—The term "data network service provider" means a person offering any service to the general public that provides the users thereof with the ability to transmit or receive data, including communications.

(6) DECRYPTION.—The term "decryption" means the retransformation or unscrambling of encrypted data, including communications, to its readable plaintext version. To "decrypt" data, including communications, is to perform decryption.

(7) DECRYPTION INFORMATION.—The term "decryption information" means information or technology that enables one to readily retransform or unscramble encrypted data from its unreadable and incomprehensible format to its readable plaintext version.

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

(9) ENCRYPTION.—The term "encryption" means the transformation or scrambling of data, including communications, from plaintext to an unreadable or incomprehensible format, regardless of the technique utilized for such transformation or scrambling and irrespective of the medium in which such data, including communications, occur or can be found, for the purposes of protecting

the content of such data, including communications. To "encrypt" data, including communications, is to perform encryption.

(10) ENCRYPTION PRODUCT.—The term "encryption product" means any software, technology, commodity, or mechanism, that can be used to encrypt or decrypt or has the capability of encrypting or decrypting any data, including communications.

(11) FOREIGN AVAILABILITY.—The term "foreign availability" has the meaning applied to foreign availability of encryption products subject to controls under the Export Administration Regulations, as in effect on July 1, 1999.

(12) GOVERNMENT.—The term "Government" means the Government of the United States and any agency or instrumentality thereof, or the government of any State, and any of its political subdivisions.

(13) INVESTIGATIVE OR LAW ENFORCEMENT OFFICER.—The term "investigative or law enforcement officer" has the meaning given that term in section 2510(7) of title 18, United States Code.

(14) NATIONAL SECURITY.—The term "national security" means the national defense, intelligence, or foreign policy interests of the United States.

(15) PLAINTEXT.—The term "plaintext" means the readable or comprehensible format of that data, including communications, which has been encrypted.

(16) PLAINVOICE.—The term "plainvoice" means communication specific plaintext.

(17) SECRETARY.—The term "Secretary" means the Secretary of Commerce, unless otherwise specifically identified.

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

(19) TELECOMMUNICATIONS CARRIER.—The term "telecommunications carrier" has the meaning given that term in section 3 of the Communications Act of 1934 (47 U.S.C. 153).

(20) TELECOMMUNICATIONS SYSTEM.—The term "telecommunications system" means any equipment, technology, or related software used in the movement, switching, interchange, transmission, reception, or internal signaling of data, including communications over wire, fiber optic, radio frequency, or any other medium.

(21) UNITED STATES PERSON.—The term "United States person" means—

(A) any citizen of the United States;

(B) any other person organized under the laws of any State; and

(C) any person organized under the laws of any foreign country who is owned or controlled by individuals or persons described in subparagraphs (A) and (B).

SEC. 102. 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 and for any United States person to use any encryption product, regardless of encryption algorithm selected, encryption bit length chosen, or implementation technique or medium used.

SEC. 103. UNLAWFUL USE OF ENCRYPTION.

(a) IN GENERAL.—Part I of title 18, United States Code, is amended by inserting after chapter 123 the following new chapter:

"CHAPTER 125—ENCRYPTED DATA, INCLUDING COMMUNICATIONS

"§ 2801. Unlawful use of encryption in furtherance of a criminal act

"(a) PROHIBITED ACTS.—Whoever knowingly uses encryption in furtherance of the commission of a criminal offense for which the person may be prosecuted in a district court of the United States shall—

"(1) in the case of a first offense under this section, be imprisoned for not more than 5 years, or fined under this title, or both; and

"(2) in the case of a second or subsequent offense under this section, be imprisoned for not more than 10 years, or fined under this title, or both.

"(b) CONSECUTIVE SENTENCE.—Notwithstanding any other provision of law, the court shall not place on probation any person convicted of a violation of this section, nor shall the term of imprisonment imposed under this section run concurrently with any other term of imprisonment imposed for the underlying criminal offense.

"(c) PROBABLE CAUSE NOT CONSTITUTED BY USE OF ENCRYPTION.—The use of encryption by itself shall not establish probable cause to believe that a crime is being or has been committed.

"§ 2802. Privacy protection

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

"(1) obtain or use decryption information without lawful authority for the purpose of decrypting data, including communications;

"(2) exceed lawful authority in decrypting data, including communications;

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

"(4) impersonate another person for the purpose of obtaining decryption information of that person without lawful authority;

"(5) facilitate or assist in the encryption of data, including communications, knowing that such data, including communications, are to be used in furtherance of a crime; or

"(6) disclose decryption information in violation of a provision of this chapter.

"(b) CRIMINAL PENALTY.—Whoever violates this section shall be imprisoned for not more than 10 years, or fined under this title, or both.

"§ 2803. Court order access to plaintext or decryption information

"(a) COURT ORDER.—(1) A court of competent jurisdiction shall issue an order, ex parte, granting an investigative or law enforcement officer timely access to the plaintext of encrypted data, including communications, or requiring any person in possession of decryption information to provide such information to a duly authorized investigative or law enforcement officer—

"(A) upon the application by an attorney for the Government that—

"(i) is made under oath or affirmation by the attorney for the Government; and

"(ii) provides a factual basis establishing the relevance that the plaintext or decryption information being sought has to a law enforcement, foreign counterintelligence, or international terrorism investigation then being conducted pursuant to lawful authorities; and

"(B) if the court finds, in writing, that the plaintext or decryption information being sought is relevant to an ongoing lawful law enforcement, foreign counterintelligence, or international terrorism investigation and the investigative or law enforcement officer is entitled to such plaintext or decryption information.

"(2) The order issued by the court under this section shall be placed under seal, except that a copy may be made available to the investigative or law enforcement officer authorized to obtain access to the plaintext of the encrypted information, or authorized to obtain the decryption information sought in the application. Such order shall, subject to the notification procedures set forth in section 2804, also be made available to the person responsible for providing the plaintext or the decryption information, pursuant to such order, to the investigative or law enforcement officer.

"(3) Disclosure of an application made, or order issued, under this section, is not authorized, except as may otherwise be specifically permitted by this section or another order of the court.

"(b) RECORD OF ACCESS REQUIRED.—(1) There shall be created an electronic record, or similar type record, of each instance in which an investigative or law enforcement officer, pursuant to an order under this section, gains access to the plaintext of otherwise encrypted information, or is provided decryption information, without the knowledge or consent of the owner of the data, including communications, who is the user of the encryption product involved.

"(2) The court issuing the order under this section may require that the electronic or similar type of record described in paragraph (1) is maintained in a place and a manner that is not within the custody or control of an investigative or law enforcement officer gaining the access or provided the decryption information. The record shall be tendered to the court, upon notice from the court.

"(3) The court receiving such electronic or similar type of record described in paragraph (1) shall make the original and a certified copy of the record available to the attorney for the Government making application under this section, and to the attorney for, or directly to, the owner of the data, including communications, who is the user of the encryption product, pursuant to the notification procedures set forth in section 2804.

"(c) AUTHORITY TO INTERCEPT COMMUNICATIONS NOT INCREASED.—Nothing in this chapter shall be construed to enlarge or modify the circumstances or procedures under which a Government entity is entitled to intercept or obtain oral, wire, or electronic communications or information.

"(d) CONSTRUCTION.—This chapter shall be strictly construed to apply only to a Government entity's ability to decrypt data, including communications, for which it has previously obtained lawful authority to intercept or obtain pursuant to other lawful authorities, which without an order issued under this section would otherwise remain encrypted.

"§ 2804. Notification procedures

"(a) IN GENERAL.—Within a reasonable time, but not later than 90 days after the filing of an application for an order under section 2803 which is granted, the court shall cause to be served, on the persons named in the order or the application, and such other parties whose decryption information or whose plaintext has been provided to an investigative or law enforcement officer pursuant to this chapter, as the court may determine is in the interest of justice, an inventory which shall include notice of—

"(1) the fact of the entry of the order or the application;

"(2) the date of the entry of the application and issuance of the order; and

"(3) the fact that the person's decryption information or plaintext data, including communications, has been provided or accessed by an investigative or law enforcement officer.

The court, upon the filing of a motion, may make available to that person or that person's counsel, for inspection, such portions of the plaintext, applications, and orders as the court determines to be in the interest of justice.

"(b) POSTPONEMENT OF INVENTORY FOR GOOD CAUSE.—(1) On an ex parte showing of good cause by an attorney for the Government to a court of competent jurisdiction, the serving of the inventory required by subsection (a) may be postponed for an additional 30 days after the granting of an order pursuant to the ex parte motion.

"(2) No more than 3 ex parte motions pursuant to paragraph (1) are authorized.

"(c) ADMISSION INTO EVIDENCE.—The content of any encrypted information that has been obtained pursuant to this chapter or evidence derived therefrom shall not be received in evidence or otherwise disclosed in any trial, hearing, or other proceeding in a Federal or State court, other than the court organized pursuant to the Foreign Intelligence Surveillance Act of 1978, unless each party, not less than 10 days before the trial, hearing, or proceeding, has been furnished with a copy of the order, and accompanying application, under which the decryption or access to plaintext was authorized or approved. This 10-day period may be waived by the court if the court finds that it was not possible to furnish the party with the information described in the preceding sentence within 10 days before the trial, hearing, or proceeding and that the party will not be prejudiced by the delay in receiving such information.

"(d) CONSTRUCTION.—The provisions of this chapter shall be construed consistent with—

"(1) the Classified Information Procedures Act (18 U.S.C. App.); and

"(2) the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.).

"(e) CONTEMPT.—Any violation of the provisions of this section may be punished by the court as a contempt thereof.

"(f) MOTION TO SUPPRESS.—Any aggrieved person in any trial, hearing, or proceeding in or before any court, department, officer, agency, regulatory body, or other authority of the United States or a State, other than the court organized pursuant to the Foreign Intelligence Surveillance Act of 1978, may move to suppress the contents of any decrypted data, including communications, obtained pursuant to this chapter, or evidence derived therefrom, on the grounds that —

"(1) the plaintext was decrypted or accessed in violation of this chapter;

"(2) the order of authorization or approval under which it was decrypted or accessed is insufficient on its face; or

"(3) the decryption was not made in conformity with the order of authorization or approval.

Such motion shall be made before the trial, hearing, or proceeding unless there was no opportunity to make such motion, or the person was not aware of the grounds of the motion. If the motion is granted, the plaintext of the decrypted data, including communications, or evidence derived therefrom, shall be treated as having been obtained in violation of this chapter. The court, upon the filing of such motion by the aggrieved person, may make available to the aggrieved person or that person's counsel for inspection such portions of the decrypted plaintext, or evidence derived therefrom, as the court determines to be in the interests of justice.

"(g) APPEAL BY UNITED STATES.—In addition to any other right to appeal, the United States shall have the right to appeal from an order granting a motion to suppress made under subsection (f), or the denial of an application for an order under section 2803, if the attorney for the Government certifies to the court or other official granting such motion or denying such application that the appeal is not taken for purposes of delay. Such appeal shall be taken within 30 days after the date the order was entered on the docket and shall be diligently prosecuted.

"(h) CIVIL ACTION FOR VIOLATION.—Except as otherwise provided in this chapter, any person described in subsection (i) may, in a civil action, recover from the United States Government the actual damages suffered by the person as a result of a violation described in that subsection, reasonable attorney's fees, and other litigation costs reasonably incurred in prosecuting such claim.

"(i) COVERED PERSONS.—Subsection (h) applies to any person whose decryption information—

"(1) is knowingly obtained without lawful authority by an investigative or law enforcement officer;

"(2) is obtained by an investigative or law enforcement officer with lawful authority and is knowingly used or disclosed by such officer unlawfully; or

"(3) is obtained by an investigative or law enforcement officer with lawful authority and whose decryption information is unlawfully used to disclose the plaintext of the data, including communications.

"(j) LIMITATION.—A civil action under subsection (h) shall be commenced not later than 2 years after the date on which the unlawful action took place, or 2 years after the date on which the claimant first discovers the violation, whichever is later.

"(k) EXCLUSIVE REMEDIES.—The remedies and sanctions described in this chapter with respect to the decryption of data, including communications, are the only judicial remedies and sanctions for violations of this chapter involving such decryptions, other than violations based on the deprivation of any rights, privileges, or immunities secured by the Constitution.

"(l) TECHNICAL ASSISTANCE BY PROVIDERS.—A provider of encryption technology or network service that has received an order issued by a court pursuant to this chapter shall provide to the investigative or law enforcement officer concerned such technical assistance as is necessary to execute the order. Such provider may, however, move the court to modify or quash the order on the ground that its assistance with respect to the decryption or access to plaintext cannot be performed in fact, or in a timely or reasonable fashion. The court, upon notice to the Government, shall decide such motion expeditiously.

"(m) REPORTS TO CONGRESS.—In May of each year, the Attorney General, or an Assistant Attorney General specifically designated by the Attorney General, shall report in writing to Congress on the number of applications made and orders entered authorizing Federal, State, and local law enforcement access to decryption information for the purposes of reading the plaintext of otherwise encrypted data, including communications, pursuant to this chapter. Such reports shall be submitted to the Committees on the Judiciary of the House of Representatives and of the Senate, and to the Permanent Select Committee on Intelligence for the House of Representatives and the Select Committee on Intelligence for the Senate.

"§ 2805. Lawful use of plaintext or decryption information

"(a) AUTHORIZED USE OF DECRYPTION INFORMATION.—

"(1) CRIMINAL INVESTIGATIONS.—An investigative or law enforcement officer to whom plaintext or decryption information is provided may only use such plaintext or decryption information for the purposes of conducting a lawful criminal investigation, foreign counterintelligence, or international terrorism investigation, and for the purposes of preparing for and prosecuting any criminal violation of law.

"(2) CIVIL REDRESS.—Any plaintext or decryption information provided under this chapter to an investigative or law enforcement officer may not be disclosed, except by court order, to any other person for use in a civil proceeding that is unrelated to a criminal investigation and prosecution for which the plaintext or decryption information is authorized under paragraph (1). Such order shall only

issue upon a showing by the party seeking disclosure that there is no alternative means of obtaining the plaintext, or decryption information, being sought and the court also finds that the interests of justice would not be served by nondisclosure.

"(b) LIMITATION.—An investigative or law enforcement officer may not use decryption information obtained under this chapter to determine the plaintext of any data, including communications, unless it has obtained lawful authority to obtain such data, including communications, under other lawful authorities.

"(c) RETURN OF DECRYPTION INFORMATION.—An attorney for the Government shall, upon the issuance of an order of a court of competent jurisdiction—

"(1)(A) return any decryption information to the person responsible for providing it to an investigative or law enforcement officer pursuant to this chapter; or

"(B) destroy such decryption information, if the court finds that the interests of justice or public safety require that such decryption information should not be returned to the provider; and

"(2) within 10 days after execution of the court's order to return or destroy the decryption information—

"(A) certify to the court that the decryption information has either been returned or destroyed consistent with the court's order; and

"(B) if applicable, notify the provider of the decryption information of the destruction of such information.

"(d) OTHER DISCLOSURE OF DECRYPTION INFORMATION.—Except as otherwise provided in section 2803, decryption information or the plaintext of otherwise encrypted data, including communications, shall not be disclosed by any person unless the disclosure is—

"(1) to the person encrypting the data, including communications, or an authorized agent thereof;

"(2) with the consent of the person encrypting the data, 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 decryption information, including determinations arising from legal proceedings associated with the incapacity, death, or dissolution of any person; or

"(5) otherwise permitted by law.

"§ 2806. Identification of decryption information

"(a) IDENTIFICATION.—To avoid inadvertent disclosure of decryption information, any person who provides decryption information to an investigative or law enforcement officer pursuant to this chapter shall specifically identify that part of the material that discloses decryption information as such.

"(b) RESPONSIBILITY OF INVESTIGATIVE OR LAW ENFORCEMENT OFFICER.—The investigative or law enforcement officer receiving any decryption information under this chapter shall maintain such information in a facility and in a method so as to reasonably assure that inadvertent disclosure does not occur.

"§ 2807. Definitions

"The definitions set forth in section 101 of the Encryption for the National Interest Act shall apply to this chapter.".

(b) CONFORMING AMENDMENT.—The table of chapters for part I of title 18, United States Code, is amended by inserting after the item relating to chapter 121 the following new item:

"125. Encrypted data, including communications ..... 2801".

TITLE II—GOVERNMENT PROCUREMENT

SEC. 201. FEDERAL PURCHASES OF ENCRYPTION PRODUCTS.

(a) DECRYPTION CAPABILITIES.—The President may, consistent with the provisions of subsection (b), direct that any encryption product or service purchased or other-

wise procured by the United States Government to provide the security service of data confidentiality for a computer system owned and operated by the United States Government shall include recoverability features or functions that enable the timely decryption of encrypted data, including communications, or timely access to plaintext by an authorized party without the knowledge or cooperation of the person using such encryption products or services.

(b) CONSISTENCY WITH INTELLIGENCE SERVICES AND MILITARY OPERATIONS.—The President shall ensure that all encryption products purchased or used by the United States Government are supportive of, and consistent with, all statutory obligations to protect sources and methods of intelligence collection and activities, and supportive of, and consistent with, those needs required for military operations and the conduct of foreign policy.

SEC. 202. NETWORKS ESTABLISHED WITH FEDERAL FUNDS.

The President may direct that any communications network established for the purpose of conducting the business of the Federal Government shall use encryption products that—

(1) include features and functions that enable the timely decryption of encrypted data, including communications, or timely access to plaintext, by an authorized party without the knowledge or cooperation of the person using such encryption products or services; and

(2) are supportive of, and consistent with, all statutory obligations to protect sources and methods of intelligence collection and activities, and supportive of, and consistent with, those needs required for military operations and the conduct of foreign policy.

SEC. 203. GOVERNMENT CONTRACT AUTHORITY.

The President may require as a condition of any contract by the Government with a private sector vendor that any encryption product used by the vendor in carrying out the provisions of the contract with the Government include features and functions that enable the timely decryption of encrypted data, including communications, or timely access to plaintext, by an authorized party without the knowledge or cooperation of the person using such encryption products or services.

SEC. 204. PRODUCT LABELS.

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

SEC. 205. NO PRIVATE MANDATE.

The United States Government may not require the use of encryption standards for the private sector except as otherwise authorized by section 204.

SEC. 206. EXCLUSION.

Nothing in this title shall apply to encryption products and services used solely for access control, authentication, integrity, nonrepudiation, digital signatures, or other similar purposes.

TITLE III—EXPORTS OF ENCRYPTION

SEC. 301. EXPORTS OF ENCRYPTION.

(a) AUTHORITY TO CONTROL EXPORTS.—The President shall control the export of all dual-use encryption products.

(b) AUTHORITY TO DENY EXPORT FOR NATIONAL SECURITY REASONS.—Notwithstanding any provision of this title, the President may deny the export of any encryption product on the basis that its export is contrary to the national security.

(c) DECISIONS NOT SUBJECT TO JUDICIAL REVIEW.—Any decision based on national security that is made by the President or his designee with respect to the export of encryption products under this title shall not be subject to judicial review.

SEC. 302. LICENSE EXCEPTION FOR CERTAIN ENCRYPTION PRODUCTS.

(a) LICENSE EXCEPTION.—Upon the enactment of this Act, any encryption product with an encryption strength of 64 bits or less shall be eligible for export under a license exception if—

(1) such encryption product is submitted for a 1-time technical review;

(2) such encryption product does not require licensing under otherwise applicable regulations;

(3) such encryption product is not intended for a country, end user, or end use that is by regulation ineligible to receive such product, and the encryption product is otherwise qualified for export;

(4) the exporter, within 180 days after the export of the product, submits a certification identifying—

(A) the intended end use of the product; and

(B) the name and address of the intended recipient of the product, where available;

(5) the exporter, within 180 days after the export of the product, provides the names and addresses of its distribution chain partners; and

(6) the exporter, at the time of submission of the product for technical review, provides proof that its distribution chain partners have contractually agreed to abide by all laws and regulations of the United States concerning the export and reexport of encryption products designed or manufactured within the United States.

(b) ONE-TIME TECHNICAL REVIEW.—(1) The technical review referred to in subsection (a) shall be completed within no longer than 45 days after the submission of all of the information required under paragraph (2).

(2) The President shall specify the information that must be submitted for the 1-time technical review referred to in this section.

(3) An encryption product may not be exported during the technical review of that product under this section.

(c) PERIODIC REVIEW OF LICENSE EXCEPTION ELIGIBILITY LEVEL.—(1) Not later than 180 days after the date of the enactment of this Act, the President shall notify the Congress of the maximum level of encryption strength, which may not be lower than 64-bit, that may be exported from the United States under license exception pursuant to this section consistent with the national security.

(2) The President shall, at the end of each successive 180-day period after the notice provided to the Congress under paragraph (1), notify the Congress of the maximum level of encryption strength, which may not be lower than that in effect under this section during that 180-day period, that may be exported from the United States under a license exception pursuant to this section consistent with the national security.

(d) FACTORS NOT TO BE CONSIDERED.—A license exception for the exports of an encryption product under this section may be allowed whether or not the product contains a method of decrypting encrypted data.

SEC. 303. DISCRETIONARY AUTHORITY.

Notwithstanding the requirements of section 305, the President may permit the export, under a license exception pursuant to the conditions of section 302, of encryption products with an encryption strength exceeding the maximum level eligible for a license exception under section 302, if the export is consistent with the national security.

SEC. 304. EXPEDITED REVIEW AUTHORITY.

The President shall establish procedures for the expedited review of commodity classification requests, or export license applications, involving encryption products that are specifically approved, by regulation, for export.

SEC. 305. ENCRYPTION LICENSES REQUIRED.

(a) UNITED STATES PRODUCTS EXCEEDING CERTAIN BIT LENGTH.—Except as permitted under section 303, in the case of all encryption products with an encryption strength exceeding the maximum level eligible for a license exception under section 302, which are designed or manufactured within the United States, the President may grant a license for export of such encryption products, under the following conditions:

(1) There shall not be any requirement, as a basis for an export license, that a product contains a method of—

(A) gaining timely access to plaintext; or

(B) gaining timely access to decryption information.

(2) The export license applicant shall submit—

(A) the product for technical review;

(B) a certification, under oath, identifying—

(i) the intended end use of the product; and

(ii) the expected end user or class of end users of the product;

(C) proof that its distribution chain partners have contractually agreed to abide by all laws and regulations of the United States concerning the export and reexport of encryption products designed or manufactured within the United States; and

(D) the names and addresses of its distribution chain partners.

(b) TECHNICAL REVIEW FOR LICENSE APPLICANTS.—(1) The technical review described in subsection (a)(3)(A) shall be completed within 45 days after the submission of all the information required under paragraph (2).

(2) The information to be submitted for the technical review shall be the same as that required to be submitted pursuant to section 302(b)(2).

(3) An encryption product may not be exported during the technical review of that product under this section.

(c) POST-EXPORT REPORTING.—

(1) UNAUTHORIZED USE.—All exporters of encryption products that are designed or manufactured within the United States shall submit a report to the Secretary at any time the exporter has reason to believe any such exported product is being diverted to a use or a user not approved at the time of export.

(2) PIRATING.—All exporters of encryption products that are designed or manufactured within the United States shall report any pirating of their technology or intellectual property to the Secretary as soon as practicable after discovery.

(3) DISTRIBUTION CHAIN PARTNERS.—All exporters of encryption products that are designed or manufactured within the United States, and all distribution chain partners of such exporters, shall submit to the Secretary a report which shall specify—

(A) the particular product sold;

(B) the name and address of—

(i) the ultimate end user of the product, if known; or

(ii) the name and address of the next purchaser in the distribution chain; and

(C) the intended use of the product sold.

(d) EXERCISE OF OTHER AUTHORITIES.—The Secretary, the Secretary of Defense, and the Secretary of State may exercise the authorities they have under other provisions of law, including the Export Administration Act of 1979, as continued in effect under the International Emergency Economic Powers Act, to carry out this title.

(e) WAIVER AUTHORITY.—

(1) IN GENERAL.—The President may by Executive order waive any provision of this title, or the applicability of any such provision to a person or entity, if the President determines that the waiver is necessary to advance the national security. The President shall, not later than 15 days after making such determination, submit a report to the committees referred to in paragraph (2) that includes the factual basis upon which such determination was made. The report may be in classified format.

(2) COMMITTEES.—The committees referred to in paragraph (1) are the Committee on International Relations, the Committee on Armed Services, and the Permanent Select Committee on Intelligence of the House of Representatives, and the Committee on Foreign Relations, the Committee on Armed Services, and the Select Committee on Intelligence of the Senate.

(3) DECISIONS NOT SUBJECT TO JUDICIAL REVIEW.—Any determination made by the President under this subsection shall not be subject to judicial review.

SEC. 306. ENCRYPTION INDUSTRY AND INFORMATION SECURITY BOARD.

(a) ENCRYPTION INDUSTRY AND INFORMATION SECURITY BOARD ESTABLISHED.—There is hereby established an Encryption Industry and Information Security Board. The Board shall undertake an advisory role for the President.

(b) PURPOSES.—The purposes of the Board are—

(1) to provide a forum to foster communication and coordination between industry and the Federal Government on matters relating to the use of encryption products;

(2) to enable the United States to effectively and continually understand the benefits and risks to its national security, law enforcement, and public safety interests by virtue of the proliferation of strong encryption on the global market;

(3) to evaluate and make recommendations regarding the further development and use of encryption;

(4) to advance the development of international standards regarding interoperability and global use of encryption products;

(5) to promote the export of encryption products manufactured in the United States;

(6) to recommend policies enhancing the security of public networks;

(7) to encourage research and development of products that will foster electronic commerce;

(8) to promote the protection of intellectual property and privacy rights of individuals using public networks; and

(9) to evaluate the availability and market share of foreign encryption products and their threat to United States industry.

(c) MEMBERSHIP.—(1) The Board shall be composed of 12 members, as follows:

(A) The Secretary, or the Secretary's designee.

(B) The Attorney General, or his or her designee.

(C) The Secretary of Defense, or the Secretary's designee.

(D) The Director of Central Intelligence, or his or her designee.

(E) The Director of the Federal Bureau of Investigation, or his or her designee.

(F) The Special Assistant to the President for National Security Affairs, or his or her designee, who shall chair the Board.

(G) Six representatives from the private sector who have expertise in the development, operation, marketing, law, or public policy relating to information security or technology. Members under this subparagraph shall each serve for 5-year terms.

(2) The six private sector representatives described in paragraph (1)(G) shall be appointed as follows:

(A) Two by the Speaker of the House of Representatives.

(B) One by the Minority Leader of the House of Representatives.

(C) Two by the Majority Leader of the Senate.

(D) One by the Minority Leader of the Senate.

(e) MEETINGS.—The Board shall meet at such times and in such places as the Secretary may prescribe, but not less frequently than every four months. The Federal Advisory Committee Act (5 U.S.C. App.) does not apply to the Board or to meetings held by the Board under this section.

(f) FINDINGS AND RECOMMENDATIONS.—The chair of the Board shall convey the findings and recommendations of the Board to the President and to the Congress within 30 days after each meeting of the Board. The recommendations of the Board are not binding upon the President.

(g) LIMITATION.—The Board shall have no authority to review any export determination made pursuant to this title.

(h) FOREIGN AVAILABILITY.—The consideration of foreign availability by the Board shall include computer software that is distributed over the Internet or advertised for sale, license, or transfer, including over-the-counter retail sales, mail order transactions, telephone order transactions, electronic distribution, or sale on approval and its comparability with United States products and its use in United States and foreign markets.

(i) TERMINATION.—This section shall cease to be effective 10 years after the date of the enactment of this Act.

TITLE IV—LIABILITY LIMITATIONS

SEC. 401. COMPLIANCE WITH COURT ORDER.

(a) NO LIABILITY FOR COMPLIANCE.—Subject to subsection (b), no civil or criminal liability under this Act, or under any other provision of law, shall attach to any person for disclosing or providing—

(1) the plaintext of encrypted data, including communications;

(2) the decryption information of such encrypted data, including communications; or

(3) technical assistance for access to the plaintext of, or decryption information for, encrypted data, including communications.

(b) EXCEPTION.—Subsection (a) shall not apply to a person who provides plaintext or decryption information to another in violation of the provisions of this Act.

SEC. 402. COMPLIANCE DEFENSE.

Compliance with the provisions of sections 2803, 2804, 2805, or 2806 of title 18, United States Code, as added by section 103(a) of this Act, or any regulations authorized by this Act, shall provide a complete defense for any civil action for damages based upon activities covered by this Act, other than an action founded on contract.

SEC. 403. GOOD FAITH DEFENSE.

An objectively reasonable reliance on the legal authority provided by this Act and the amendments made by this Act, authorizing access to the plaintext of otherwise encrypted data, including communications, or to decryption information that will

allow the timely decryption of data, including communications, that is otherwise encrypted, shall be an affirmative defense to any criminal or civil action that may be brought under the laws of the United States or any State.

TITLE V—INTERNATIONAL AGREEMENTS

SEC. 501. SENSE OF CONGRESS.

It is the sense of Congress that—

(1) the President should conduct negotiations with foreign governments for the purposes of establishing binding export control requirements on strong non-recoverable encryption products; and

(2) such agreements should safeguard the privacy of the citizens of the United States, prevent economic espionage, and enhance the information security needs of the United States.

SEC. 502. FAILURE TO NEGOTIATE.

The President may consider a government's refusal to negotiate agreements described in section 501 when considering the participation of the United States in any cooperation or assistance program with that country.

SEC. 503. REPORT TO CONGRESS.

(a) REPORT TO CONGRESS.—The President shall report annually to the Congress on the status of the international effort outlined by section 501.

(b) FIRST REPORT.—The first report required under subsection (a) shall be submitted in unclassified form no later than September 1, 2000.

TITLE VI—MISCELLANEOUS PROVISIONS

SEC. 601. EFFECT ON LAW ENFORCEMENT ACTIVITIES.

(a) COLLECTION OF INFORMATION BY ATTORNEY GENERAL.—The Attorney General shall compile, and maintain in classified form, data on—

(1) the instances in which encryption has interfered with, impeded, or obstructed the ability of the Department of Justice to enforce the laws of the United States; and

(2) the instances where the Department of Justice has been successful in overcoming any encryption encountered in an investigation.

(b) AVAILABILITY OF INFORMATION TO THE CONGRESS.—The information compiled under subsection (a), including an unclassified summary thereof, shall be submitted to Congress annually beginning October 1, 2000.

SEC. 602. INTERPRETATION.

Nothing contained in this Act or the amendments made by this Act shall be deemed to—

(1) preempt or otherwise affect the application of the Arms Export Control Act (22 U.S.C. 2751 et seq.), the Export Administration Act of 1979 (50 U.S.C. App. 2401 et seq.), or the International Emergency Economic Powers Act (50 U.S.C. 1701 et seq.) or any regulations promulgated thereunder;

(2) affect foreign intelligence activities of the United States; or

(3) negate or diminish any intellectual property protections under the laws of the United States or of any State.

SEC. 603. FBI TECHNICAL SUPPORT.

There are authorized to be appropriated for the Technical Support Center in the Federal Bureau of Investigation, established pursuant to section 811(a)(1) of the Antiterrorism and Effective Death Penalty Act of 1996 (Public Law 104–132)—

(1) $25,000,000 for fiscal year 2000 for building and personnel costs;

(2) $20,000,000 for fiscal year 2001 for personnel and equipment costs;

(3) $15,000,000 for fiscal year 2002; and

(4) $15,000,000 for fiscal year 2003.

SEC. 604. SEVERABILITY.

If any provision of this Act or the amendments made by this Act, or the application thereof, to any person or circumstances is held invalid by a court of the United States, the remainder of this Act or such amendments, and the application thereof, to other persons or circumstances shall not be affected thereby.

PURPOSE

The House Permanent Select Committee on Intelligence sought referral of H.R. 850, the "Security and Freedom through Encryption (SAFE) Act," as reported by the House Committee on the Judiciary, because the bill impacts directly upon matters relating to the intelligence and intelligence-related activities and national security capabilities of the Intelligence Community. Specifically, the bill will have a profound effect on the intelligence, counter-intelligence, and counter-terrorism responsibilities of the Department of Defense, the National Security Agency, the Department of Justice, and the Federal Bureau of Investigation, to name but a few of those Intelligence Community agencies within this Committee's jurisdiction. The legislation as introduced or reported by the Committees on the Judiciary, International Relations, and Commerce, raises serious issues of great significance to our national security and public safety. Because of the significant risk to the intelligence and intelligence-related activities and capabilities of the United States the Committee determined that it needed to act in a comprehensive manner.

The paramount duty of government is to protect its citizens from harm to their persons or property. Fundamental to a free society, however, is a delicate balance between the need to defend the nation's security and preserving the liberties of the people endowed by their Creator. The balance achieved in the Constitution and the Bill of Rights provides a clear backdrop against which the Committee's legislative action should be considered.

During the Committee's consideration of H.R. 850 it was determined that the SAFE Act did not adequately address the national security and public safety interests at stake in the public policy debate over encryption legislation. Government official, after government official, advised the Committee that strong encryption is being used to facilitate drug trafficking, child pornography, terrorism, espionage, and myriad other crimes. Proponents of the SAFE Act urged the Committee to ignore the concern of these witnesses and to leave the management of encryption policy to the marketplace. They argued that it was too late to do anything about the widespread use of strong encryption. They asserted that the "genie was out of the bottle" and could not be put back in. They claimed that any effort to continue control of encryption technology would be a losing proposition that would harm industry. They rejected the enormous consequences described by the government officials charged with the duty to protect the national security and defend the public safety.

The Committee considered the arguments of the SAFE Act proponents and the administration officials and struck a balance. The Committee's amendment, the "Encryption for the National Interest Act," gives the government the authority:

- To access the plaintext of encrypted information, through the use of court orders, during lawful criminal, foreign intelligence, and international terrorist investigations;
- To control encryption exports in defense of the national security;

- To procure and use encryption products with recoverability features; and
- To improve their technical capabilities against the widespread use of strong encryption.

But, at the same time, the Encryption for the National Interest Act assures the industry and the cyber-libertarians that their concerns have too been heeded. The bill provides that:

- U.S. persons can use any encryption product of any strength regardless of whether it contains access to plaintext capabilities;
- All access to plaintext or decryption information will be upon the order of a judge after an appropriate showing by the government;
- Civil and criminal sanctions can be imposed upon those who misuse the decryption information of any other person; and
- Electronic audit trails are required whenever law enforcement accesses the plaintext or decryption information of an encryption user.

The Encryption for the National Interest Act asserts that the nation's security and the protection of its citizens are worthy objectives of the federal government and its principal obligation. The Encryption for the National Interest Act also, however, seeks to establish a dynamic and constructive framework for continued cooperation between government and industry to achieve a workable solution to this extremely vexing issue facing the nation. It does not preclude continued American competitiveness in an increasingly competitive global market, yet secures the right of the Commander-in-Chief to defend our interests against those who wish us harm. It does not turn national security and public security over to the random behavior of the marketplace.

The Encryption for the National Interest Act achieves a compromise in the best interests of all protagonists in this public debate: industry, national security, public safety, and privacy. The Committee's amendment was adopted upon a unanimous voice vote of the Committee, and H.R. 850 was ordered reported favorably to the House, as amended by the Committee.

SUMMARY

SECTION-BY-SECTION ANALYSIS

Section 1.—Short title and table of contents

This section provides the title of the bill as the "Encryption for the National Interest Act" and a table of contents.

Section 2.—Statement of policy

This section sets forth the policy of the United States with respect to encryption technology.

Section 3.—Congressional findings

This section sets forth the findings of Congress as to the important role information security technology, encryption, plays in relaying and protecting intelligence information, linking policy makers, establishing an effective foreign policy, protecting United

States banking and financial systems and critical infrastructure, and citizens from such crimes as fraud, theft, drug trafficking, espionage, terrorism, money laundering, and child pornography, among other serious offenses.

TITLE I—DOMESTIC USE OF ENCRYPTION

Section 101.—Definitions

This section establishes the definitions of specific terms used throughout the bill.

Section 102.—Lawful use of encryption

This section makes clear that, except as otherwise provided, it is lawful to use encryption products, regardless of algorithm length selected, encryption key length chosen, or implementation technique or medium used.

Section 103.—Unlawful use of encryption

This section amends Title 18, United States Code, by new sections 2801 through 2807 within new chapter 122, which bears the heading, "Chapter 122–Encrypted Data, Including Communications."

New section 2801 of Title 18, United States Code, would make it a criminal offense to use encryption in furtherance of the commission of a federal crime. The penalties attached to such crimes would be in addition to any sentence imposed for the underlying offense. For first time offenders, a fine under Title 18, United States Code, or both. For repeat offenders of this provision, the jail time is potentially no more than 10 years. This section also makes clear that merely using encryption, without additional facts, cannot be the basis for a probable cause determination.

New section 2802 creates several new crimes. First, it makes it illegal to intentionally obtain or use decryption information without lawful authority in order to decrypt data, including information. In addition, it makes it a criminal offense to exceed lawful authority in decrypting data, including communications. This new section would make the breaking of encryption code of another without lawful authority and with the purpose of violating that person's privacy or security, or for the purpose of depriving that person of his or her property a criminal violation of law. Furthermore this section would make it a criminal offense to assist in the encryption of data knowing that such data, including communications are to be used in furtherance of a crime.

New section 2803 sets forth the standards and procedures for the issuance of a court order granting an investigative or law enforcement officer timely access to the plaintext of otherwise encrypted data, including communications, or compelling the provision of decryption information to an investigative or law enforcement officer that has a lawful basis to obtain that data. The application for such order must be made by an attorney for the government. That application must establish facts supporting the finding that the plaintext of decrypted information is relevant to an on-going lawful law enforcement, foreign counterintelligence, or international terrorist investigation. The application and any order issued thereon

shall be made ex parte and placed under seal. Disclosure of the application or order is not authorized, except as may be otherwise permitted by this section or another order of the court.

This section also requires that the court granting access to plaintext or the disclosure of decryption information, shall also ensure that a verifiable audit trail of any access to plaintext or decrypted information be maintained.

The record will be tendered to the court upon an order of the court.

Subsection (d) clarifies that nothing in this new chapter shall be read to expand or modify any other constitutional or statutory requirement under which a government entity is entitled to intercept or obtain oral, wire, or electronic communications or information.

Subsection (e) mandates a strict construction of this new chapter so that it is read only to apply to a government entity's ability to decrypt or otherwise gain access to the plaintext data, including communications, for which it previously obtained lawful authority to intercept or obtain.

New section 2804 provides the users of encryption products with a statutory right to be notified when their decryption information is provided to law enforcement, or when law enforcement is granted access to the plaintext of their data, including communications. This section provides for a delayed notification to the user so as not to jeopardize the integrity of the on-going criminal investigation, foreign counterintelligence, or international terrorist investigation. Basically, the user must be notified within 90 days after the filing of an application for the decryption information, or for access to the plaintext, unless the judge finds good cause warranting delay. Specifically, however, neither any of the decrypted contents of the encrypted information that has been obtained, nor any evidence derived therefrom may be used in any proceeding unless the user has been furnished with a copy of the order, application, and the data, including communications. The user may move to suppress the use of any of the plaintext or evidence derived therefrom in any proceeding on the grounds that the plaintext or the decryption information was unlawfully obtained. This section also provides aggrieved persons with a civil cause of action for any violations of this new chapter.

New section 2805 limits the lawful uses of plaintext or decryption information obtained under this chapter. It may be used for the purposes of conducting a lawful criminal or foreign counterintelligence or terrorist investigation and for the purposes of preparing for and prosecuting any criminal violation of law. It may not be disclosed to any party to a civil suit that does not arise from criminal investigation or prosecution, unless a court finds that there is no alternative means of obtaining the plaintext, or decryption information and that the interests of justice would not be served by nondisclosure. This section further clarifies that decryption information may not be used to determine the plaintext unless the officer possesses other lawful authority to plaintext.

This section also outlines the procedures for returning or destroying any decryption information upon the conclusion of the investigation, trial, or proceeding. This section also places limitations upon any person acting as a key recovery agent. It specifies whom

and under what circumstances a key recovery agent may provide decryption information to another person.

New section 2806 requires those who are providing decryption information to an investigative or law enforcement officer to so identify that information in order to avoid any inadvertent disclosure. The officer is responsible for maintaining the decryption information in such a manner so as reasonably to ensure against inadvertent disclosure.

New section 2807 states that the same definitions set forth in section 101 of the "Encryption for the National Interest Act" shall apply to this chapter.

TITLE II—GOVERNMENT PROCUREMENT

Section 201.—Federal purchases of encryption products

This section permits the United States government to purchase encryption products enabling the timely decryption by an authorized party, without the knowledge or cooperation of the person using the encryption product. This requirement only applies to those products or services purchased or procured by the United States government for data confidentiality for computer systems armed or operated by the United States.

The Committee believes that a "National Information Assurance Plan" is needed to ensure that the data, including communications, of the United States government are secure. To this end the Committee requests that the President submit to the Permanent Select Committee on Intelligence and the Committee on Armed Services of the House of Representatives and the Select Committee on Intelligence and the Committee on Armed Services of the Senate within 120 days after enactment of this Act a report that outlines the national information assurance plan and policy for the United States government.

The Committee believes that any plan or policy developed should include the following goals, which should be addressed in the report to be submitted to the congressional committees:

(1) The protection of the Federal Government's information infrastructure against hostile penetration by ensuring the Federal Government's use of the strongest possible information assurance products, including encryption, in secure configurations and applications;

(2) A requirement that the Federal Government use products designed or manufactured in the United States enabling the recovery of information pursuant to lawful authority; and

(3) A requirement that the Federal Government use reliable authentication products designed or manufactured in the United States so that the Federal Government knows who is accessing its systems.

Section 202.—Networks established with federal funds

This section permits the President to require that any communications network that is established for the purpose of conducting the business of the Federal Government must use encryption products that include techniques enabling the timely decryption of data, including communications, without the knowledge or cooperation of

the person using the encryption product or service. It is not intended that private communications networks that might benefit from federal grants fall within this requirement. Nor is it intended that this section include the Internet, although it is understood that there may be government business that is conducted via the Internet.

Section 203.—Government contract authority

This section grants to the President of the United States the authority to require, as a condition of any contract by the United States government with a private vendor that any encryption product used by the vendor in carrying out the provisions of the contract include features and functions that enable the decryption of encrypted data, including communications, or timely access to plaintext by an authorized party without the knowledge or cooperation of the person using such encryption products or services.

Section 204.—Product labels

This section allows for the labeling of encryption products so that purchasers and users are aware that the product is authorized for sale to, or for use in transactions with, the United States government.

Section 205.—No private mandate

This section specifies that the United States government may not require the use of encryption standards for the private sector except as otherwise authorized by section 203.

Section 206.—Exclusion

This section clarifies that nothing in this title shall apply to encryption products and services used solely for access control, authentication, integrity, non-repudiation, digital signatures, or other similar purposes.

TITLE III—EXPORTS OF ENCRYPTION

Section 301.—Exports of encryption

Subsection (a) authorizes the President to control the export of all dual-use encryption products.

Subsection (b) grants the President the authority to deny the export of any encryption product on the basis that its exportation would be contrary to the national security interests of the United States.

Subsection (c) specifies that all national security decisions made by the President, or his designee, under this title shall not be subject to judicial review.

Section 302.—License exception for certain encryption products

Subsection (a) sets forth criteria for the export of those encryption products with an encryption strength of 64 bits or less under a license exception. The product must be submitted for a 1-time technical review, not require licensing under otherwise applicable regulations, and not be intended for a country, end-user, or end use that is otherwise ineligible to receive such products. In ad-

dition, the exporter must within six months after export supply the names and addresses of its distribution chain partners, and identify the intended end user (if available) or use of the product. The exporter must provide proof that its distribution chain partners have contractually agreed to abide by all laws and regulations of the United States regarding export and re-export of encryption products.

Subsection (b) sets a time limit of 45 days after submission for all information required for the technical review for the completion of the review referred to in subsection (a).

Subsection (c) requires that the President notify Congress every six months of the maximum strength level encryption that may be exported under a license exception pursuant to this section without harm to national security. The initial maximum bit level for which products can be exported under this exception shall not be less than 64 bits. This brings U.S. policy in line with Waasenaar Arrangement commitments. At the end of each successive 180-day period, the President shall notify Congress of the maximum encryption bit level that may be exported under license exception. The levels cannot be reduced once raised by the President. This report will ensure that the Administration review on a regular, short-term basis, which is necessary given the dynamic nature of technology, the appropriate level to allow products out under a license exception.

Subsection (d) enables the export of a product under a license exception that meets the criteria set forth in section 302(a), regardless of whether the product contains a method of decrypting encrypted data. There is no requirement that recoverability features be included in the product for this section to apply.

Section 303.—Discretionary authority

Section 303 authorizes the President to allow the export, under a license exception, of encryption products with bit lengths greater than that level set through operation of section 302, subject to the conditions of section 302, if the export would be consistent with the national security interest of the United States.

This provision ensures that export of those 128-bit encryption products currently allowed under a license exception may continue after enactment of the Act.

Section 304.—Expedited authority

This section grants the President authority to establish procedures for expediting the review of commodity classification requests, or export license applications involving encryption products that are specifically approved, by regulation, for export.

Section 305.—Encryption licenses required

Subsection (a) establishes criteria the President shall employ in the review and granting of a license for export of encryption products exceeding the maximum level eligible for license exception under section 302. Products being considered for export determinations shall not be required to contain features or functions for the timely access to plaintext or decryption information. In addition, any bit length encryption product is eligible for export under this

section. The license applicant is responsible for submitting the product for technical review, certifying under oath the intended end user, the end use of the product, and providing the names and addresses of its distribution chain partners. The exporter must certify that these distributors are contractually obligated to abide by all laws and regulations of the United States concerning the export and re-export of encryption products and services.

Subsection (b) further clarifies that the technical review described in subsection (a) to be completed within 45 days after product submission and no export shall occur during the technical review.

Subsection (c) sets forth post-export reporting requirements to be submitted to the Secretary of Commerce. Reports shall be filed specifically when the exporter believes the exported encryption products or services are being diverted to a user or use not approved for export, or the exporter has detected pirating of their technology or intellectual property. In addition, all exporters and their distribution chain partners shall report the names and addresses of the next purchaser in the distribution chain.

Subsection (d) clarifies that the Secretaries of Commerce, Defense, and State may exercise the authority they have under other provisions of law, specifically the International Emergency Economic Powers Act.

Subsection (e) provides the President with the authority to waive any provision of this title for national security purposes. Requires the President to report to the relevant committees of Congress within 15 days after this authority is used. The determination made by the President shall not be subject to judicial review.

Section 306.—Encryption industry and information security board

This section establishes an Encryption Industry and Information Security Board ("EIIS") to advise the President on future encryption policy and technological advancements that might serve to alter the United States policy on encryption products. This section also defines the purposes of the board. It further specifies that the Board shall be composed of 12 members, and how those members shall be appointed. In addition to the Secretary of Commerce, Secretary of Defense, Attorney General, the Director of Central Intelligence, the Director of the Federal Bureau of Investigation, and the Special Assistant to the President for National Security Affairs, or their designees; six representatives from the private sector who have expertise in development, operation, marketing, law, and public policy relating to information security or technology shall be appointed by Congressional Leadership. The Board will have no authority to challenge or review an export determination made pursuant to this Act. The Board will report to the President and the Congress. This section will cease to be effective 10 years after the date of enactment.

TITLE IV—LIABILITY LIMITATIONS

Section 401.—Compliance with court order

This section states that a person shall not be subject to civil or criminal liability under this Act, or under any other provision of

law, for acting in compliance with a court order compelling the disclosure of plaintext or decryption information.

Section 402.—Compliance defense

This section provides a complete defense for any non-contract action for damages based upon activities covered by the Act as long as the person complies with the provisions of sections 2803, 2804, 2805, and 2806 of Title 18, United States Code, as amended by section 103(a) of this Act, or any regulations authorized by this Act.

Section 403.—Good faith defense

This section provides anyone who relies on the legal authority provided under this Act as the basis for providing an investigative or law enforcement officer with access to the plaintext of otherwise encrypted data, including communications, or for providing such officer with decryption information, a complete defense to any criminal or civil action arising therefrom.

TITLE V—INTERNATIONAL AGREEMENTS

Section 501.—Sense of Congress

This section expresses the Sense of Congress that the President should negotiate with foreign governments to establish binding export control requirements on nonrecoverable encryption products. Any agreement should safeguard the privacy of U.S. persons, prevent economic espionage, and enhance the information security needs of the United States.

Section 502.—Failure to negotiate

This section permits the President to take a country's refusal to negotiate into consideration when making decisions about U.S. participation in any cooperation or assistance program with that country.

Section 503.—Report to Congress

This section requires an annual report to Congress on the status of the negotiations, with the first report due September 1, 2000.

TITLE VI—MISCELLANEOUS PROVISIONS

Section 601.—Effect on law enforcement activities

This section requires the Attorney General to compile, and maintain in classified form, information on those instances where encryption has posed problems in the enforcement of federal laws. This information will be available to any Member of Congress upon request.

Section 602.—Interpretation

This section clarifies the relationship of the bill to the interpretation of certain laws: the bill does not preempt the application of other important export control acts, including: the Arms Export Control Act, the Export Administration Act, or the International Emergency Powers Act. It shall not affect foreign intelligence activities of the United States; nor does it diminish the intellectual

property protections provided by the laws of the U.S. or of any State.

Section 603.—FBI technical support

This section authorizes appropriations totaling $75 million for fiscal years 2000 through 2003 to the Federal Bureau of Investigation for the Technical Support Center established pursuant to section 811(a)(1) of the Antiterrorism and Effective Death Penalty Act of 1996. (P.L. 104–132)

Section 604.—Severability

This section permits any court reviewing this Act to sever any provision from the remainder of the Act, so as not to find the Act invalid in its entirety.

BACKGROUND AND NEED FOR LEGISLATION

BENEFITS OF STRONG ENCRYPTION

There is little doubt that strong encryption has enormous benefits for society. For our national security apparatus, it is invaluable and essential to secure the flow of intelligence information, enhance our ability to execute foreign policy, and ensure the protection of the 1.4 million men and women of our armed forces deployed around the world. It is fundamental to protecting the Nation's critical infrastructures, such as power grids, telecommunications, and transportation facilities. Strong encryption is a remarkable tool that has aided the advancement of the Internet. It has been one factor in the explosive growth of on-line commerce, banking, investments, telemedicine, and legal services, to name only a few areas where the Internet has changed our daily lives.

Encryption also advances the interests of law enforcement where it is used for legitimate purposes, because it can and does shield on-line activities from criminals interested in stealing personal financial data, credit card information, or national secrets, for example. But, as crucial as it is to the protection of information, it can be equally harmful to our Nation's security and the public's safety.

PROBLEMS WITH H.R. 850, AS REFERRED TO THE COMMITTEE

After all, the benefit that strong encryption provides to the individual legitimate encryption user is equally provided to the person with criminal intent. Our laws should not preclude lawful investigation of criminal activity. Our laws should enhance the Nation's security and public safety. The SAFE Act (H.R. 850), as reported by the Committee on the Judiciary, would deny law enforcement authorities the opportunity to obtain evidence—evidence to which they are statutorily authorized to obtain—simply because a criminal decided to encrypt it. Under that bill, the child pornographer will be able to operate with impunity. The terrorist will be able to communicate with his comrades. He will be able to plan and execute his cowardly acts without fear that he will be identified or brought to justice. Spies would operate without fear of discovery. The drug trafficker will be able to arrange for distribution of his poison and collection of the thousands or millions of dollars made in the deal. He will be able to launder his proceeds unconcerned

that his activities have caught the attention of the law enforcement authorities. Those that engage in the proliferation of weapons of mass destruction will be able to continue their menacing activities unhindered by our national security apparatus or intelligence collectors.

Allowing the unchecked export of unbreakable encryption to all markets and all users across the globe presents a series of challenges that the national security agencies of the United States cannot meet or overcome simply by employing faster and more powerful computers. The consequences of such a policy would be devastating. Criminals and international thugs wishing to do harm to the people of the United States would have available to them an "electronic sanctuary."

Legislation that precludes the federal government from using encryption products that permit the recovery of data or communications is irresponsible. The SAFE Act has been read to do just this. With the time it would take to break just one 128-bit encrypted message (many times the age of the universe), annihilation would be quicker than our ability to protect ourselves.

Without an ability to undo quickly an encryption code, the people of this country could suffer unfathomable harm. Similarly, child pornographers could distribute their filth unimpeded. Pedophiles could secretly entice the children of America into their clutches. Drug traffickers will make their plans to deliver larger and larger amounts of cocaine, heroin, marijuana, and other narcotics without the slightest concern that they will be detected. Terrorists and spies can cause unspeakable damage without even the possibility of being stopped before it is too late. In a world governed by policies espoused by the SAFE Act, protecting America, her interests, and her citizens becomes a far riskier endeavor.

While the SAFE Act does not on its face remove export controls, the regime it would establish is so fraught with exceptions and limitations on government authority that control might as well be nonexistent. The SAFE Act does acknowledge, however, that the nation's security should override an ability to export on occasion. Yet, the circumstances under which the SAFE Act would authorize denial of exports are limited only to those instances where the Secretary of Commerce has "substantial evidence" that the product intended for export was going to Iran, Iraq, North Korea, Libya, Sudan, Cuba, and Syria, or has "substantial evidence" that a specific product would be used by foreign militaries or terrorists. First, there is no role under the SAFE Act for the participation of the national security apparatus of the United States in such decisions not to export. Secondly, there can be no doubt that these two factors cover only a fraction of all situations that present threats to our national security interests. A broader authority to deny exports must be provided in order to ensure the nation's security in an age of constantly changing political realities.

Expert witnesses before the Committee and Congress have provided compelling and sobering testimony about the lack of balance in H.R. 850 as reported from the Judiciary Committee. The administration opposes any encryption legislation that is not balanced. "The current version [of H.R. 850] does not balance the needs of privacy and business, public safety, and national security, * * *."

Testimony of Janet Reno, Attorney General of the United States, before the House Permanent Select Committee on Intelligence on July 14, 1999. "The proposed SAFE Act does not include any provisions aimed at improving law enforcement's ability to perform its public safety mission in an encrypted world." Id. "The objective of the legislation is unfettered encryption which has no concern for public safety and, in all reality, eliminates any concerns for public safety in the future." Testimony of Thomas A. Constantine, former Administrator, Drug Enforcement Administration, before the House Permanent Select Committee on Intelligence on July 14, 1999 (hereinafter "Constantine Test."). "The [SAFE Act] * * * will harm law enforcement, will harm public safety, will harm national security, and lives will be lost * * *." Testimony of Louis J. Freeh, Director, Federal Bureau of Investigation, before the House Committee on Armed Services on July 13, 1999. "[R]ather than a SAFE Act * * * I would call it the 'Drug Lords Protection Act.'" Constantine Test. "[T]he SAFE Act will harm national security by making [NSA's] job of providing critical, actionable intelligence to our leaders and military commanders difficult, if not impossible, thus putting our nation's security at considerable risk." Testimony of Barbara A. McNamara, Deputy Director, National Security Agency, before the House Committee on Armed Services on July 13, 1999. "H.R. 850 * * * would be a tidal wave that would crush your national security and law enforcement agencies that are protecting this country." Testimony of John J. Hamre, Deputy Secretary, Department of Defense, before the House Committee on Armed Services on July 13, 1999. "[T]here are real national security and law enforcement costs to the policy that is articulated by the [SAFE Act]. * * *" Testimony of William Reinsch, Undersecretary of Commerce for Export Administration, Department of Commerce (hereinafter "Reinsch Test."), before the House Committee on Armed Services on July 13, 1999. "[T]he bill in letter and spirit would destroy the balance we have worked so hard to achieve and would jeopardize our law enforcement and national security interests." Reinsch Test. before the House Permanent Select Committee on Intelligence on June 9, 1999.

Importantly, during his appearance before the HPSCI on June 9, 1999, Mr. Goodlatte, the author of the SAFE Act, conceded that a balance needed to be achieved on this issue. Mr. Goodlatte stated that he shared the serious national security and law enforcement concerns at stake in this debate. Testimony of Representative Bob Goodlatte (hereinafter "Goodlatte Test.") before the House Permanent Select Committee on Intelligence on June 9, 1999, at pp. 26, 27, 28, 52. He claimed his bill was not designed to eliminate all export controls, which was a significant concession. Goodlatte Test. at pp. 21, 30. It is a testament to the notion that we cannot place market share and larger profits ahead of the nation's security and the public's safety. It further reemphasizes the concept that there must be accommodation in the encryption export control policy to assure the national security and the interests of the industry. Mr. Goodlatte's support for export controls in certain circumstances extends to the foundational concept that export controls can be used to protect against threats to the national security of the United States. Goodlatte Test. at pp. 31, 44. He also testified that it was

not the intent of his legislation to deny law enforcement the ability to gain access to plaintext or decryption information, where it was available. Goodlatte Test. at pp. 34, 53, 77. See also Report of the Committee on the Judiciary to Accompany H.R. 850, House Report 106–117, Part 1, at p. 8 (April 27, 1999) ("Just as new technology should not take away the longstanding rights of citizens against government, it also should not take away the traditional means for legitimate law enforcement and national security investigations.") He was open to modification of the "substantial evidence" standard his bill uses to preclude an export of encryption to terrorists and militaries in order to alleviate the risks attendant to the export of encryption throughout the world. Goodlatte Test. at pp. 38, 43, 44. He further contended that it was not the intent of his legislative proposal to preclude the federal government, or state and local governments, from using encryption products that have features or functions that permit the recovery of data when those government entities find it necessary to use such products. Goodlatte Test. at pp. 77. Although not included anywhere in his legislation, Mr. Goodlatte also supports the provision of more and better resources to federal, state, and local law enforcement so they can more adequately meet the challenges of widespread use of strong encryption. Goodlatte Test. at pp. 25, 28, 53, 54.

BALANCED APPROACH IS NEEDED

The HPSCI reported amendment, the "Encryption for the National Interest Act," strives to balance the needs of law enforcement, national security, industry, and privacy. It advances the interests of all sectors engaged in this debate, yet requires some sacrifice on the part of each, as well.

The Committee amendment preserves law enforcement's crime fighting and public safety capabilities by providing clear authority through judicial processes to access the plaintext or decryption information, without the target of the investigation's knowledge or cooperation. It does not, however, require key escrow, or mandate key recovery. Key recovery is a non-factor for domestic use and for export considerations.

In addition to laying the framework for a national information assurance program, the Committee's amendment will relax the current export control policy of the United States on encryption products to bring the policy in line with the government's commitments under the Waasenaar Arrangement. In other words, where now only those products of 56-bit strength and lower can be exported under a license exception, upon enactment of the HPSCI amendment, all products of 64-bit strength and lower will be allowed for export in this manner. All products in excess of 64-bits will require a license prior to export, unless granted a waiver. This will permit the export of any bit-length encryption product under license exception conditions to those sectors that pose little or no risk to national security. Of course, prior to the first export of any encryption product, the Committee's amendment will still require a technical review to be conducted.

Furthermore, the Committee's amendment requires the administration to review its encryption export policies on a more regularized basis than is currently done. The amendment requires a semi-

annual look at export policy and certifications to Congress with respect to the results of this review.

The Committee's amendment also streamlines export reporting requirements in an effort to reduce the burdensome and costly paperwork that is the bane of the industry. It does not remove these requirements completely, as the SAFE Act does, because there is significant national security utility in such reporting and the Committee determined it should continue in some form.

Importantly, the Encryption for the National Interest Act preserves the President's authority to protect national security by authorizing him, or his designee, to deny an export of an encryption product based on national security grounds. This is an acknowledgement that the conduct of foreign policy and the protection of the citizens of the United States cannot be tied to only a couple of particular threats. The exigencies of our role as the world's only superpower must be accommodated and our export control regime must reflect the need for such flexibility.

The Committee's amendment permits the federal government to procure and utilize encryption products with recoverability features for the conduct of the government's business. Likewise, the federal government will be permitted to require that its contractors use recoverable encryption products for the conduct of the government's business pursuant to the government contract. This authority does not permit, however, the government to require contractors to use such products in the course of their private sector, non-governmental business activities.

Finally, the Committee's amendment establishes an advisory board to assist the President in his determination of appropriate encryption export policies and to foster government-industry cooperation on this important issue with significant ramifications for national security and public safety. Moreover, the Committee's legislative initiative authorizes the appropriation of $75 million to build, equip, and maintain the FBI's Technical Support Center. This Center will help move law enforcement at all levels forward in this age of high technology. It will help law enforcement meet and overcome the substantial challenges presented in a world where strong encryption will be commonplace.

The Committee's Ranking Democrat, Representative Julian C. Dixon, put the matter succinctly after the Committee adopted its amendment in the nature of a substitute, when he stated:

> The encryption compromise adopted by the Intelligence Committee achieves two important goals: it recognizes that government access to information on the electronic infrastructure—when necessary to protect public safety and national security—is legitimate within reasonable, lawful constraints; and, it provides greater certainty in the export control process while allowing for regulatory flexibility as technology advances. The balance between commercial interests and public safety achieved by the Intelligence Committee substitute has improved greatly the encryption legislation with which the Committee was asked to deal.

The Committee believes that the United States government should encourage the development of encryption products that are

responsive to the needs and obligations of government to ensure public safety, and that are viable in the commercial marketplace, without resorting to mandated key recovery or key escrow. For certain, law enforcement would have no difficulty obtaining decrypted evidence of criminality were Congress to impose mandatory requirements on the encryption industry to develop products with access to plaintext functions or features. Such an approach, however, does not advance the debate on comprehensive encryption policy for the United States in the fast approaching 21st Century.

The Committee determined that the SAFE Act, as reported by the Judiciary, the International Relations, and the Commerce Committees did not adequately address national security and public safety concerns. In fact, the Committee found, based on the testimony of various witnesses before the Committee, that the SAFE Act actually would disadvantage our national security apparatus and federal, state, and local law enforcement in the conduct of their very serious obligations. To correct these faults, the Committee decided that an amendment in the nature of a substitute was necessary rather than merely "tinkering around the edges" of the SAFE Act, in order to ensure that the appropriate and desired balance could be achieved. Thus, the Committee adopted by unanimous voice vote the "Encryption for the National Interest Act."

THE "ENCRYPTION FOR THE NATIONAL INTEREST ACT"

A. Establishes government encryption procurement policies

As noted, the Committee amendment, the Encryption for the National Interest Act, permits the United States government to procure and use encryption products that include recoverability or comparable features to allow authorized parties to have access to plaintext. The SAFE Act forbids the government and the States from using such products; and the SAFE Act would deny the government the opportunity to encourage the development of products with features that might help catch spies, thieves, child pornographers, and embezzlers, among others. Thus, specifically, the Encryption for the National Interest Act would authorize the United States government to include as a condition of any government contract a requirement that any encryption employed by the contractor in the execution of the contract with the government will include features permitting access to plaintext or decryption information. This amendment would not require that federal government contractors use recoverable encryption products in the conduct of non-federal government business. The Committee amendment also does not preclude the States from employing recoverable encryption products. The SAFE Act, however, includes such a prohibition.

B. Preserves law enforcement's investigative capabilities

The Encryption for the National Interest Act also establishes definite procedures to be followed by federal, state, and local law enforcement when seeking access to the plaintext or decryption information of data, including communications, that is otherwise encrypted. Without expanding current wiretap or search and seizure authorities, the amendment allows law enforcement, through

judicially authorized court orders, to gain access to decryption information, or to plaintext, where it is available, for use in criminal, foreign counterintelligence, and international terrorism investigations. A close reading of the SAFE Act would deny law enforcement this critical capability. The SAFE Act would deny law enforcement the ability to decrypt any encrypted communications that are intercepted through legitimate court issued wiretap orders.

Many proponents of the SAFE Act routinely assert that wiretaps are of limited utility to law enforcement, and that the lack of this capability would cause no egregious harm to public safety. The Committee's extensive experience and the testimony on this matter indicate otherwise.

Some have concluded that the effort to enact the SAFE Act is a not-so- subtle attempt to render the government's wiretap authority void. As the distinguished Chairman of the House Committee on the Judiciary, Chairman Henry Hyde wrote in October 1996, "Without a remedy, America will effectively disarm itself of one of its most potent weapons in the fight against two particularly pernicious crimes: international terrorism and drug smuggling." Washington Times, p. B3, October 27, 1996. Mr. Hyde made the point that "efforts to prevent or eliminate this important law enforcement tool are both naïe and dangerous." Id. He concluded, by asserting, "Our Constitution requires the federal government to provide for the common security of the people. Wiretaps, used sparingly and with court authorization, are indispensable in safeguarding both our liberties and our security in an age of dangerous uncertainty." Id. Although Chairman Hyde was expressing his concern about digital telephony, his logic and arguments are entirely apt within the context of this public debate over encryption policy, and should be heeded.

C. Protects civil liberties

It is apparent to the Committee that the use of encryption to protect the security of one's data or communications would be indicative of an individual's heightened expectation of privacy with respect to that data or communication. Although this does not raise the search and seizure probable cause standard of the Fourth Amendment to the Constitution of the United States, Congress can provide additional procedural protections that will recognize this heightened expectation of privacy. In fact, the Encryption for the National Interest Act does exactly this while allowing law enforcement agencies to conduct their investigations in this computer age. The Committee amendment provides a judicially supervised mechanism for accessing the plaintext or decryption information. It likewise permits all U.S. persons to purchase and use any encryption technology that is available anywhere in the world, whether it contains access to plaintext capabilities, or not.

Most proponents of the SAFE Act speak of the need to protect our privacy from the "abuses" of government, particularly law enforcement. They assert that any access capability to the plaintext of communications or stored data will leave law abiding Americans vulnerable to government prying and abusive intrusion into our private lives. In making these claims, the supporters of the SAFE

Act ignore the bulwark of our freedoms, the guarantor of our liberties: the Constitution.

The Framers, brilliant in their foresight, understood that—at times—there might happen an occasion where government misunderstood its mission, where government intruded on the liberties of its citizenry. It was due to this foresight that the Constitution requires neutral, detached magistrates to approve the search or seizure of the people's papers and effects. The judicial branch protects the people from the excesses of the state. We cannot forget that there are lawful processes to redress abuses that might be committed. But, simply because speculative abuses might occur at some unknown time in the future under unknowable circumstances is no reason to deny law enforcement the legal authority to obtain evidence of criminal activity that might be encrypted today. The Committee's amendment, in an effort to further encourage the appropriate handling of one's decryption information, permits civil and criminal sanctions for those who exceed their lawful authority, who misuse the information, or who violate any provision of title I of the Act.

D. Maintains but streamlines export controls on encryption products

The Committee believes that increased market share for United States industry is a societal good that should be supported, and that trends in market share for U.S. information technology products should be one factor—but only one factor—in the design of export controls for sensitive technologies. Providing tools to our malefactors, who want to invade our privacy and confound our law enforcement or intelligence professionals, makes no sense at any price. Thus, any legislation on encryption policy must be balanced. Unfortunately, some in the information technology industry have argued that anything short of the Judiciary Committee's approach to encryption export control legislation is unacceptable.

The Encryption for the National Interest Act maintains a meaningful export control regime that places national security as the premium interest to be considered when contemplating the export of strong encryption products from the United States. But, at the same time, it relaxes current export control policies where appropriate and streamlines end use and end user reporting. Although it authorizes the President to control exports of encryption products, and to deny an export on national security grounds, it allows for more products to be exported under license exceptions and under specially granted Presidential waivers for products above 64–bit length strength. It also requires the executive branch to more routinely review the level at which products can be exported by license exception. This will add regularity to what has been described as an inconsistent method by which the executive branch has reviewed encryption export control policy.

The current policy was issued nearly one year ago, and many believe it was only produced as a result of pressure brought to bear upon the executive branch by the industry and Congress. This seems to be an ad hoc method of addressing a critical national security issue of this magnitude. So, the Committee amendment attempts to inject order into the regulatory process and to create a dynamic and constructive regulatory structure that will address

the needs of industry, though not losing sight of the serious national security and public safety implications of any export of encryption products.

The Intelligence Committee amendment seeks to lighten this burdensome responsibility for industry while at the same time obtaining important national security information. The Encryption for the National Interest Act provides for a meaningful technical review period that will provide the United States government with an opportunity to make well informed and rational national security determinations under the Act, when necessary. Additionally, the Committee amendment would eliminate recoverability features as a condition for export; indeed, the amendment would eliminate recovery features as a factor in reaching any export determination.

The Encryption for the National Interest Act does not try to return the proverbial "genie to the bottle," but rather merely seeks to manage the spread of encryption in a manner that is consistent with national security and public safety interests and in a way that will foster the continued dominance of the American encryption industry in the global marketplace. The Committee believes it would be a mistake of catastrophic proportions to allow indecipherable encryption to be exported without restriction. Public safety and national security are not matters that should be left to the ebb and flow of technological advances and breakthroughs, or to the random fluctuations of the marketplace.

It is important to note that no one doubts that U.S. manufactured encryption products are facing competition from foreign providers. But, simply because a product of purported capability is available in a country with dubious reliability at controlling terrorists or drug traffickers, for instance, is not a sufficient reason for removing virtually all limitations on the export of encryption of the strongest sort. Rather, it seems it would be wise for the President to consider whether U.S. industry stands to lose market share in a particular market if not permitted to export to that market and whether export to that market sector presents undue risks to the national security. It cannot be overstated: the Committee shares the concern of American industry that its products could be replaced by foreign competitors. It notes, however, that the grip of the U.S. industry on the global market is truly remarkable. Testimony before the Committee indicates U.S. industry controls approximately 75–80% of the global encryption market. Goodlatte Test. at p. 50. This "full-nelson" hold by U.S. encryption manufacturers and designers on the global market is noteworthy given what many have described as restrictive export controls. On this point, it is worth highlighting that in 1997 only 25 of 1,850 applications for encryption export licenses were denied; in 1998, the numbers were 13 of 1,895; and thus far in 1999, only 1 of 508 applications has been denied.

Interesting to note, too, is that despite the alarmist rhetoric put forward in support of the SAFE Act, to wit: "many hundreds of thousands of American jobs are at stake here," see Goodlatte Test. at p. 32, Congress last year authorized an additional 50,000 nonimmigrant H–1B work visas, P.L. 105–277, because there are not enough Americans with the skills needed to fill the available computer industry jobs. Similarly, Congress is currently debating an-

other increase to the number of H–1B work visas to be allowed. The claims that hundred of thousands of American jobs are at risk appears to be a bit of hyperbole.

Moreover, all sides of this issue acknowledge that U.S. encryption technology is the best in the world. There is no wish on the part of the Committee to undermine that position, nor diminish the U.S. preeminence in this regard. Indeed, it is the national security interest for U.S. industry to dominate this market, but only under proper circumstances and with the appropriate degree of regulation.

CONCLUSION

The encryption policy of the United States requires a comprehensive approach that takes into account the interests of national security; federal, state, and local law enforcement; industry; and the citizens of the United States. The Committee's amendment in the nature of a substitute to H.R. 850 as reported by the Committee on the Judiciary, renamed by the amendment as the Encryption for the National Interest Act, strikes the well-measured balance that so many have sought since this national policy debate began.

COMMITTEE PROCEEDINGS

The Committee met several times in executive session where it was briefed on the topic of encryption and the serious national security and public safety consequences resulting from pending encryption legislation. Witnesses before the Committee at these briefings included: the President's Special Envoy on Encryption Policy, Ambassador David Aaron; the Honorable Louis J. Freeh, Director, Federal Bureau of Investigation; the Honorable Thomas A. Constantine, Administrator, Drug Enforcement Administration; the Honorable John J. Hamre, Deputy Secretary of Defense; and the Honorable Barbara A. McNamara, Deputy Director, National Security Agency.

The Committee held three closed briefings for Members of the Committee and three hearings on H.R. 850. The first briefing was held on June 8, 1999. That was followed by the first hearing, which was held on June 9, 1999, in open session. The second hearing was held on June 15, 1999, in closed session. The second briefing was held on June 16, 1999. The final briefing was held on July 13, 1999. The final hearing was held July 14, 1999, in open session.

On June 8, 1999, the Deputy Director of the NSA, the Honorable Barbara A. McNamara, briefed the Members of the Committee in closed session on the equities of the intelligence community that are impacted by the SAFE Act.

Witnesses before the Committee at the June 9, 1999, hearing were: the Honorable Bob Goodlatte, United States Representative, 6th District of Virginia, and author of the "Security and Freedom through Encryption (SAFE) Act" (H.R. 80); the Honorable William Reinsch, Under Secretary, Bureau of Export Administration, Department of Commerce; Mr. Christopher G. Caine, Vice President of Governmental Affairs, IBM Corporation; Ms. Elizabeth Kaufman, Senior Director and General Manager for Security, Cisco Systems, Inc.; Colonel Michael D. Robinson, First Vice President,

International Association of Chiefs of Police (IACP); Mr. Alan Davidson, Counsel, Center for Democracy and Technology; Mr. Ramon Marks, Board Member, Business Executives for National Security (BENS); the Honorable John Kaye, former President, National District Attorney's Association; Mr. Richard D. Heideman, President, B'nai B'rith International. In addition to this testimony presented live to the Committee, the following submissions for the record were also received and considered: Statement of Jeffrey H. Smith, Counsel, Americans for Computer Privacy; Statement of Security Dynamics Technologies, Inc.; and the Statement of Mr. Patrick P. Gelsinger, Vice President for Desktop Productions, Intel Corporation.

At the June 15, 1999, closed hearing on H.R. 850, the Committee took testimony from the Honorable Louis J. Freeh, Director, Federal Bureau of Investigation; the Honorable Thomas A. Constantine, Administrator, Drug Enforcement Administration; and the Honorable John J. Hamre, Deputy Secretary of Defense.

On June 16, 1999, the Members of the Committee were briefed by the President's Special Envoy for Encryption Policy, Ambassador David Aaron, on the administration's efforts to achieve international agreement or consensus on the appropriate approach to encryption policy and export controls.

Members of the Committee received another briefing on July 13, 1999, from the Honorable Barbara A. McNamara, Deputy Director of NSA, concerning the SAFE Act. The focus of the briefing included the effect of removal of export controls on national security and intelligence, as well as questions surrounding the issue of foreign availability and foreign market share.

The witnesses appearing before the Committee at the July 14, 1999, open hearing were: the Honorable Janet Reno, Attorney General of the United States; the Honorable Louis J. Freeh, Director, Federal Bureau of Investigation; Thomas A. Constantine, former Administrator of the Drug Enforcement Administration; and the Honorable John J. Hamre, Deputy Secretary of Defense.

The Committee extensively reviewed additional testimony, reports, and other written materials relating to encryption policy in general, and H.R. 850 in particular. Among the documents reviewed by the Committee are House Report 106–117, Part 1, Committee on the Judiciary Report on H.R. 850, April 27, 1999; House Report 106–117, Part 2, Committee on Commerce Report on H.R. 850, July 2, 1999; Senate Report 106–48, Senate Select Committee on Intelligence Report on Fiscal S. 1009, the Intelligence Authorization Act for Fiscal Year 2000, May 11, 1999; House Report 105–108, Part 1, Committee on the Judiciary Report on H.R. 695, May 22, 1997; House Report 105–108, Part 2, Committee on International Relations Report on H.R. 695, July 25, 1997; House Report 105–108, Part 3, Committee on National Security Report on H.R. 65, September 12, 1997; House Report 105–108, Part 4, Permanent Select Committee on Intelligence Report on H.R. 695, September 16, 1997; House Report 105–108, Part 5, Committee on Commerce Report on H.R. 695, September 29, 1997; Hiding Crimes in Cyberspace, Dorothy E. Denning and William E. Baugh, Jr., to appear in Information, Communication and Society, vol. 2, no. 3 (Autumn 1999) and in Cybercrime, B.D. Loader and D. Thomas (eds.)

Routledge, 1999; Growing Development of Foreign Encryption Products in the Face of U.S. Export Regulations, Lance J. Hoffman, et al, Cyberspace Policy Institute, School of Engineering and Applied Science, George Washington University, Washington, D.C., June 1999; Cryptography & Liberty 1999: An International Survey of Encryption Policy, Electronic Privacy Information Center, Washington, DC, June 1999; Congressional Research Service Issue Brief Encryption Technology: Congressional Issues, produced by Mr. Richard M. Nunno, February 25, 1999; Terrorism in the Next Millennium: Enter the Cyberterrorist, by George R. Barth, National Counterintelligence Center; Access With Trust, Federal Public Key Infrastructure Steering Committee, Government Information Technology Services Board, Office of Management and Budget, Washington, DC, September 1998; Cryptography Policy: the Guidelines and the Issues, Organization for Economic Cooperation and Development, Washington, DC, March 1998; Deciphering the Cryptography Debate, by Kenneth Flamm, The Brookings Institution; The Risks of Key Recovery, Key Escrow, & Trusted Third Party Encryption: A Report by an Ad Hoc Group of Cryptographers and Computer Scientists, produced by Center for Democracy and Technology, June 1998; "Opening the Lines for Criminal Conversation," Robert D. Novak, Washington Post, June 28, 1999; and "Wiretap Technology. Updating an effective tool," by the Honorable Henry J. Hyde, Washington Times, October 1996.

Testimony before the United States House of Representative Judiciary Subcommittee on Courts and Intellectual Property, March 4, 1999: The Honorable William A. Reinsch, Under Secretary for Export Administration, Department of Commerce; Mr. Dave McCurdy, President, Electronic Industries Alliance; the Honorable Ron Lee, Associate Deputy Attorney General, Department of Justice; Mr. Craig McLaughlin, Chief Technology Officer, Privada, Inc.; Mr. Edward Gillespie, Executive Director, Americans for Computer Privacy; Mr. Thomas Parenty, Director, Data and Communications Security Sybase, Inc. on behalf of Business Software Alliance; Ms. Dorothy E. Denning, Computer Science Department, Georgetown University; and Statement of the Honorable Howard Coble, United States Representative, 6th District of North Carolina.

Testimony before the United States House of Representatives Commerce Subcommittee on Telecommunications Trade and Consumer Protection, May 25, 1999: The Honorable Ronald D. Lee, Associate Deputy Attorney General, Department of Justice; the Honorable Barbara A. McNamara, Deputy Director, National Security Agency; the Honorable William A. Reinsch, Undersecretary Bureau of Export Administration, Department of Commerce, Executive Director, Americans for Computer Privacy; Mr. Richard Hornstein, General Counsel, Network Associates; Mr. Tom Arnold, Vice President and Chief Technology Officer, CyberSource Corporation; Dr. Gene Schultz, Trusted Security Advisor, Global Integrity Corporation; Mr. Paddy Holohan, Executive Vice President, Marketing, Baltimore Technologies International Finance Services Centre; and Mr. David Dawson, Chairman and CEO, V-One Corporation.

Testimony before the United States House of Representatives Armed Services Committee, July 13, 1999: the Honorable Janet Reno, Attorney General; the Honorable William A. Reinsch, Under-

secretary for Export Administration, Department of Commerce; the Honorable Louis J. Freeh, Director, Federal Bureau of Investigation; Ms. Elizabeth Kaufman, Senior Director and General Manager for Security, Cisco Systems, Inc; and Mr. Matthew Bowcock, Executive Vice President of Cooperate Development, Baltimore Technologies.

In addition, the Committee staff was briefed on the subject of encryption from representatives of Cisco Systems, Inc.; IBM; Nortel; 3Com; Center for Technology and Democracy; Netscape; Motorola; the Alliance for Network Security; the Business Software Alliance; and Americans for Computer Privacy.

COMMITTEE CONSIDERATION

The Committee met on July 15, 1999, to mark up H.R. 850. In closed session, the Committee approved by unanimous voice vote the amendment in the nature of a substitute to H.R. 850 as amended and reported by the Committee on the Judiciary (House Report No. 106–117, Part 1, (April 27, 1999)), which was offered by Chairman Goss and Mr. Dixon and further amended by Ms. Pelosi. Upon adoption of the Goss and Dixon amendment as amended, the Committee, in open session, by unanimous voice vote, ordered H.R. 850, the "Encryption for the National Interest Act," as amended by the Committee, reported favorably to the House, a quorum being present.

VOTE OF THE COMMITTEE

During its consideration of H.R. 850, the Committee took no roll call votes.

FINDINGS AND RECOMMENDATIONS OF THE COMMITTEE ON GOVERNMENT REFORM AND OVERSIGHT

With respect to clause 3(c)(4) of rule XIII of the Rules of the House of Representatives, the Committee has not received a report from the Committee on Government Reform pertaining to the subject of the bill.

OVERSIGHT FINDINGS

In compliance with clause 3(c)(1) of rule XIII of the Rules of the House of Representatives, the bill as reported by the Committee reflects the conclusions, findings, and recommendations of the Committee in light of its oversight activity.

CONGRESSIONAL BUDGET OFFICE ESTIMATES

In compliance with clause 3(c)(2) and (3) of rule XIII of the Rules of the House of Representatives, and pursuant to sections 308 and 402 of the Congressional Budget Act of 1974, the Committee submits the following estimate prepared by the Congressional Budget Office:

U.S. CONGRESS,
CONGRESSIONAL BUDGET OFFICE,
Washington, DC, July 23, 1999.

Hon. PORTER J. GOSS,
Chairman, Committee on Intelligence, House of Representatives, Washington, DC.

DEAR MR. CHAIRMAN: The Congressional Budget Office has prepared the enclosed cost estimate for H.R. 850, the Encryption for the National Interest Act.

If you wish further details on this estimate, we will be pleased to provide them. The CBO staff contacts are Mark Hadley and Mark Grabowicz.

Sincerely,

BARRY B. ANDERSON
(For Dan L. Crippen, Director).

Enclosure.

H.R. 850—Encryption for the National Interest Act

Summary: H.R. 850 would clarify the President's authority to control the export of encryption products. The effectiveness or strength of contemporary encryption products is measured by the number of bits that make up the key for the encryption algorithm. (The term "key" refers to the mathematical code used to translate encrypted information back into its original, unencrypted format.) Under current policy, domestic producers may export encryption products with key lengths of up to 56 bits and stronger products for specified industries.

H.R. 850 would generally allow domestic producers to export encryption products with key lengths of up to 64 bits. The President would determine the maximum strength of encryption products that may be exported (with a review and potential update of that maximum every 180 days). The bill would establish a board to advise the President on the export of encryption products. H.R. 850 also would establish two federal crimes relating to the improper use of encryption technology and would require the Attorney General to issue numerous reports and maintain data on the instances in which encryption impedes or obstructs the ability of the Department of Justice (DOJ) to enforce the criminal laws. Finally, the bill would authorize appropriations of $75 million over the 2000–2003 period to establish a technical support center within the Federal Bureau of Investigation (FBI).

Assuming the appropriation of the necessary amounts, CBO estimates that enacting this bill would result in additional discretionary spending by DOJ of about $80 million over the 2000–2004 period. Enacting H.R. 850 also would affect direct spending and receipts. Therefore, pay-as-you-go procedures would apply. CBO estimates, however, that the amounts of additional direct spending and receipts would not be significant.

CBO is uncertain whether H.R. 850 contains intergovernmental mandates as defined in the Unfunded Mandates Reform Act (UMRA), but we estimate that any costs to state, local, or tribal governments would not be significant and would not meet the

threshold established by that act ($50 million in 1996, adjusted annually for inflation).

This bill would impose no new private-sector mandates as defined in UMRA.

Estimated cost to the Federal Government: The estimated budgetary impact of H.R. 850 is shown in the following table. For purpose of this estimate, CBO assumes H.R. 850 will be enacted by the beginning of fiscal year 2000 and that the authorized amounts will be provided for each year. The costs of this legislation fall within budget function 750 (administration of justice).

	By fiscal years, in millions of dollars—				
	2000	2001	2002	2003	2004
SPENDING SUBJECT TO APPROPRIATION					
Estimated Authorization Level	26	21	16	16	1
Estimated Outlays	19	25	16	16	4

BASIS OF ESTIMATE

Spending subject to appropriation

H.R. 850 would establish a technical support center within the FBI and authorize appropriations of $75 million over the 2000–2003 period. Based on the historical spending patterns of FBI funds, CBO estimates that implementing this provision would result in outlays of $74 million over the 2000–2004 period.

In addition, CBO estimates that complying with the bill's data collection and reporting requirements would cost DOJ about $1 million a year, assuming appropriation of the necessary amounts. The expense of compiling and maintaining data on the instances in which encryption impedes or obstructs the ability of the department to enforce the criminal laws is difficult to ascertain because the number of such instances is unknown—but DOJ believes that if H.R. 850 were enacted they would be numerous.

Under current policy, the Department of Commerce's (DOC's) Bureau of Export Administration (BXA) would likely spend about $500,000 a year reviewing exports of encryption products. If H.R. 850 were enacted, BXA would still be required to review requests to export encryption products. Thus, CBO estimates that implementing H.R. 850 would not significantly change the costs to control exports of nonmilitary encryption products.

H.R. 850 would establish a new federal crime for using encryption technologies to conceal incriminating information relating to a felony from law enforcement officials and for illegally decrypting private information. The bill would also create a new federal crime for violating privacy by decrypting someone's private information. Because H.R. 850 would establish new federal crimes, CBO anticipates that the U.S. government would be able to pursue cases that it otherwise would be unable to prosecute. Based on information from DOJ, however, we do not expect the government to pursue many additional cases. Thus, CBO estimates that implementing these provisions would not have a significant impact on the cost of federal law enforcement activity.

Direct spending and revenues

Enacting H.R. 850 would affect direct spending and receipts by imposing criminal fines. Collections of such fines are recorded in the budget as governmental receipts (i.e., revenues), which are deposited in the Crime Victims Fund and spent in subsequent years. Any additional collections as a result of this bill are likely to be negligible, however, because the federal government would probably not pursue many cases under the bill. Because any increase in direct spending would equal the fines collected (with a lag of one year or more), the additional direct spending would be negligible.

Direct spending also could result from the provision that would allow the government to be sued for decrypting private information without a court order. CBO expects that this provision is not likely to result in any significant spending.

Pay-as-you-go considerations: The Balanced Budget and Emergency Control Act sets up pay-as-you-go procedures for legislation affecting direct spending or receipts. H.R. 850 would affect direct spending and receipts by imposing criminal fines and by allowing civil actions against the United States government. CBO estimates that the amount of additional direct spending and receipts would not be significant.

Estimated impact on State, local, and tribal governments: H.R. 850 would require state and local law enforcement agencies to follow specified procedures in order to obtain access to the decryption keys of suspected criminals and would require state courts to undertake additional administrative duties in processing such requests. In addition, the bill would limit the liability of anyone who provides access to a decryption key to law enforcement officials who follow the procedures prescribed by the bill. We cannot determine if the requirements of H.R. 850 would constitute new intergovernmental mandates because it is unclear how these requirements would interact with the current wiretap, search, and seizure laws. CBO estimates that the costs of those requirements would be small because they are similar to current laws and procedures and because the burden of the bill's requirements would fall predominantly on federal entities. We therefore estimate that the bill would not impose significant costs on state, local, or tribal governments and that such costs would not exceed the threshold established by UMRA ($50 million in 1996), adjusted annually for inflation.)

Estimated impact on the private sector: This bill would impose no new private-sector mandates as defined in UMRA.

Previous CBO estimates: CBO has completed numerous other estimates of bills affecting the export of encryption products, including three versions of H.R. 850. Differences between this estimate and our previous estimates reflect differences between the bills. On April 21, 1999, CBO transmitted a cost estimate for H.R. 850 as ordered reported by the House Committee on the Judiciary on March 24, 1999. On July 1, 1999, CBO transmitted an estimate for H.R. 850 as ordered reported by the House Committee on Commerce on June 23, 1999. On July 16, 1999, CBO transmitted an estimate of H.R. 850 as ordered reported by the House Committee on International Relations on July 13, 1999. On July 9, 1999, CBO transmitted an estimate for S. 798, the Promote Online Trans-

actions to Encourage Commerce and Trade (PROTECT) Act of 1999, as ordered reported by the Senate Committee on Commerce, Science, and Transportation on June 23, 1999. And on July 22, 1999, CBO transmitted an estimate for H.R. 850 as ordered reported by the House Committee on Armed Services on July 21, 1999.

CBO estimated that the versions of H.R. 850 reported by the Judiciary Committee and the International Relations Committee would each cost between $3 million and $5 million over the 2000–2004 period, that the version reported by the Armed Services Committee would cost $5 million over the 2000–2004 period, and that the House Commerce Committee's version of H.R. 850 and the Senate bill (S. 798) would each increase costs by at least $25 million over the same period. None of those previously estimated bills contain authorizations for a new technical support center within the FBI.

Estimate prepared by: Federal costs: Mark Hadley and Mark Grabowicz. Impact on State, local, and tribal governments: Shelley Finlayson.

Estimate approved by: Robert A. Sunshine, Deputy Assistant Director for Budget Analysis.

COMMITTEE COST ESTIMATES

The Committee agrees with the estimate of the Congressional Budget Office.

SPECIFIC CONSTITUTIONAL AUTHORITY FOR CONGRESSIONAL ENACTMENT OF THIS LEGISLATION

The intelligence and intelligence-related activities of the United States government are carried out to support the national security interests of the United States, to support and assist the armed forces of the United States, and to support the President in the execution of the foreign policy of the United States. Article 1, section 8, of the Constitution of the United States provides, in pertinent part, that "Congress shall have power * * * to pay the debts and provide for the common defense and general welfare of the United States; * * * "; "to raise and support Armies, * * * "; "to provide and maintain a Navy; * * * " and "to make all laws which shall be necessary and proper for the carrying into execution . . . all other powers vested by this Constitution in the Government of the United States, or in any Department or Officer thereof." Therefore, pursuant to such authority, Congress is empowered to enact this legislation.

CHANGES IN EXISTING LAW MADE BY THE BILL, AS REPORTED

In compliance with clause 3(e) of rule XIII of the Rules of the House of Representatives, changes in existing law made by the bill, as reported, are shown as follows (existing law proposed to be omitted is enclosed in black brackets, new matter is printed in italic, existing law in which no change is proposed is shown in roman):

TITLE 18, UNITED STATES CODE

* * * * * * *

* * * * * * *

CHAPTER 125—ENCRYPTED DATA, INCLUDING COMMUNICATIONS

§ 2801. Unlawful use of encryption in furtherance of a criminal act

(a) PROHIBITED ACTS.—Whoever knowingly uses encryption in furtherance of the commission of a criminal offense for which the person may be prosecuted in a district court of the United States shall—

(1) in the case of a first offense under this section, be imprisoned for not more than 5 years, or fined under this title, or both; and

(2) in the case of a second or subsequent offense under this section, be imprisoned for not more than 10 years, or fined under this title, or both.

(b) CONSECUTIVE SENTENCE.—Notwithstanding any other provision of law, the court shall not place on probation any person convicted of a violation of this section, nor shall the term of imprisonment imposed under this section run concurrently with any other term of imprisonment imposed for the underlying criminal offense.

(c) PROBABLE CAUSE NOT CONSTITUTED BY USE OF ENCRYPTION.—The use of encryption by itself shall not establish probable cause to believe that a crime is being or has been committed.

§ 2802. Privacy protection

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

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

(2) exceed lawful authority in decrypting data, including communications;

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

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

(5) facilitate or assist in the encryption of data, including communications, knowing that such data, including communications, are to be used in furtherance of a crime; or

(6) disclose decryption information in violation of a provision of this chapter.

(b) CRIMINAL PENALTY.—Whoever violates this section shall be imprisoned for not more than 10 years, or fined under this title, or both.

§ 2803. Court order access to plaintext or decryption information

(a) COURT ORDER.—(1) A court of competent jurisdiction shall issue an order, ex parte, granting an investigative or law enforcement officer timely access to the plaintext of encrypted data, including communications, or requiring any person in possession of decryption information to provide such information to a duly authorized investigative or law enforcement officer—

(A) upon the application by an attorney for the Government that—

(i) is made under oath or affirmation by the attorney for the Government; and

(ii) provides a factual basis establishing the relevance that the plaintext or decryption information being sought has to a law enforcement, foreign counterintelligence, or international terrorism investigation then being conducted pursuant to lawful authorities; and

(B) if the court finds, in writing, that the plaintext or decryption information being sought is relevant to an ongoing lawful law enforcement, foreign counterintelligence, or international terrorism investigation and the investigative or law enforcement officer is entitled to such plaintext or decryption information.

(2) The order issued by the court under this section shall be placed under seal, except that a copy may be made available to the investigative or law enforcement officer authorized to obtain access to the plaintext of the encrypted information, or authorized to obtain the decryption information sought in the application. Such order shall, subject to the notification procedures set forth in section 2804, also be made available to the person responsible for providing the plaintext or the decryption information, pursuant to such order, to the investigative or law enforcement officer.

(3) Disclosure of an application made, or order issued, under this section, is not authorized, except as may otherwise be specifically permitted by this section or another order of the court.

(b) RECORD OF ACCESS REQUIRED.—(1) There shall be created an electronic record, or similar type record, of each instance in which an investigative or law enforcement officer, pursuant to an order under this section, gains access to the plaintext of otherwise encrypted information, or is provided decryption information, without the knowledge or consent of the owner of the data, including communications, who is the user of the encryption product involved.

(2) The court issuing the order under this section may require that the electronic or similar type of record described in paragraph (1) is maintained in a place and a manner that is not within the

custody or control of an investigative or law enforcement officer gaining the access or provided the decryption information. The record shall be tendered to the court, upon notice from the court.

(3) The court receiving such electronic or similar type of record described in paragraph (1) shall make the original and a certified copy of the record available to the attorney for the Government making application under this section, and to the attorney for, or directly to, the owner of the data, including communications, who is the user of the encryption product, pursuant to the notification procedures set forth in section 2804.

(c) AUTHORITY TO INTERCEPT COMMUNICATIONS NOT INCREASED.—Nothing in this chapter shall be construed to enlarge or modify the circumstances or procedures under which a Government entity is entitled to intercept or obtain oral, wire, or electronic communications or information.

(d) CONSTRUCTION.—This chapter shall be strictly construed to apply only to a Government entity's ability to decrypt data, including communications, for which it has previously obtained lawful authority to intercept or obtain pursuant to other lawful authorities, which without an order issued under this section would otherwise remain encrypted.

§ 2804. Notification procedures

(a) IN GENERAL.—Within a reasonable time, but not later than 90 days after the filing of an application for an order under section 2803 which is granted, the court shall cause to be served, on the persons named in the order or the application, and such other parties whose decryption information or whose plaintext has been provided to an investigative or law enforcement officer pursuant to this chapter, as the court may determine is in the interest of justice, an inventory which shall include notice of—

(1) the fact of the entry of the order or the application;

(2) the date of the entry of the application and issuance of the order; and

(3) the fact that the person's decryption information or plaintext data, including communications, has been provided or accessed by an investigative or law enforcement officer.

The court, upon the filing of a motion, may make available to that person or that person's counsel, for inspection, such portions of the plaintext, applications, and orders as the court determines to be in the interest of justice.

(b) POSTPONEMENT OF INVENTORY FOR GOOD CAUSE.—(1) On an ex parte showing of good cause by an attorney for the Government to a court of competent jurisdiction, the serving of the inventory required by subsection (a) may be postponed for an additional 30 days after the granting of an order pursuant to the ex parte motion.

(2) No more than 3 ex parte motions pursuant to paragraph (1) are authorized.

(c) ADMISSION INTO EVIDENCE.—The content of any encrypted information that has been obtained pursuant to this chapter or evidence derived therefrom shall not be received in evidence or otherwise disclosed in any trial, hearing, or other proceeding in a Federal or State court, other than the court organized pursuant to the Foreign Intelligence Surveillance Act of 1978, unless each party, not

less than 10 days before the trial, hearing, or proceeding, has been furnished with a copy of the order, and accompanying application, under which the decryption or access to plaintext was authorized or approved. This 10-day period may be waived by the court if the court finds that it was not possible to furnish the party with the information described in the preceding sentence within 10 days before the trial, hearing, or proceeding and that the party will not be prejudiced by the delay in receiving such information.

(d) CONSTRUCTION.—The provisions of this chapter shall be construed consistent with—

(1) the Classified Information Procedures Act (18 U.S.C. App.); and

(2) the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.).

(e) CONTEMPT.—Any violation of the provisions of this section may be punished by the court as a contempt thereof.

(f) MOTION TO SUPPRESS.—Any aggrieved person in any trial, hearing, or proceeding in or before any court, department, officer, agency, regulatory body, or other authority of the United States or a State, other than the court organized pursuant to the Foreign Intelligence Surveillance Act of 1978, may move to suppress the contents of any decrypted data, including communications, obtained pursuant to this chapter, or evidence derived therefrom, on the grounds that—

(1) the plaintext was decrypted or accessed in violation of this chapter;

(2) the order of authorization or approval under which it was decrypted or accessed is insufficient on its face; or

(3) the decryption was not made in conformity with the order of authorization or approval.

Such motion shall be made before the trial, hearing, or proceeding unless there was no opportunity to make such motion, or the person was not aware of the grounds of the motion. If the motion is granted, the plaintext of the decrypted data, including communications, or evidence derived therefrom, shall be treated as having been obtained in violation of this chapter. The court, upon the filing of such motion by the aggrieved person, may make available to the aggrieved person or that person's counsel for inspection such portions of the decrypted plaintext, or evidence derived therefrom, as the court determines to be in the interests of justice.

(g) APPEAL BY UNITED STATES.—In addition to any other right to appeal, the United States shall have the right to appeal from an order granting a motion to suppress made under subsection (f), or the denial of an application for an order under section 2803, if the attorney for the Government certifies to the court or other official granting such motion or denying such application that the appeal is not taken for purposes of delay. Such appeal shall be taken within 30 days after the date the order was entered on the docket and shall be diligently prosecuted.

(h) CIVIL ACTION FOR VIOLATION.—Except as otherwise provided in this chapter, any person described in subsection (i) may, in a civil action, recover from the United States Government the actual damages suffered by the person as a result of a violation described in

that subsection, reasonable attorney's fees, and other litigation costs reasonably incurred in prosecuting such claim.

(i) COVERED PERSONS.—Subsection (h) applies to any person whose decryption information—

(1) is knowingly obtained without lawful authority by an investigative or law enforcement officer;

(2) is obtained by an investigative or law enforcement officer with lawful authority and is knowingly used or disclosed by such officer unlawfully; or

(3) is obtained by an investigative or law enforcement officer with lawful authority and whose decryption information is unlawfully used to disclose the plaintext of the data, including communications.

(j) LIMITATION.—A civil action under subsection (h) shall be commenced not later than 2 years after the date on which the unlawful action took place, or 2 years after the date on which the claimant first discovers the violation, whichever is later.

(k) EXCLUSIVE REMEDIES.—The remedies and sanctions described in this chapter with respect to the decryption of data, including communications, are the only judicial remedies and sanctions for violations of this chapter involving such decryptions, other than violations based on the deprivation of any rights, privileges, or immunities secured by the Constitution.

(l) TECHNICAL ASSISTANCE BY PROVIDERS.—A provider of encryption technology or network service that has received an order issued by a court pursuant to this chapter shall provide to the investigative or law enforcement officer concerned such technical assistance as is necessary to execute the order. Such provider may, however, move the court to modify or quash the order on the ground that its assistance with respect to the decryption or access to plaintext cannot be performed in fact, or in a timely or reasonable fashion. The court, upon notice to the Government, shall decide such motion expeditiously.

(m) REPORTS TO CONGRESS.—In May of each year, the Attorney General, or an Assistant Attorney General specifically designated by the Attorney General, shall report in writing to Congress on the number of applications made and orders entered authorizing Federal, State, and local law enforcement access to decryption information for the purposes of reading the plaintext of otherwise encrypted data, including communications, pursuant to this chapter. Such reports shall be submitted to the Committees on the Judiciary of the House of Representatives and of the Senate, and to the Permanent Select Committee on Intelligence for the House of Representatives and the Select Committee on Intelligence for the Senate.

§ 2805. Lawful use of plaintext or decryption information

(a) AUTHORIZED USE OF DECRYPTION INFORMATION.—

(1) CRIMINAL INVESTIGATIONS.—An investigative or law enforcement officer to whom plaintext or decryption information is provided may only use such plaintext or decryption information for the purposes of conducting a lawful criminal investigation, foreign counterintelligence, or international terrorism investigation, and for the purposes of preparing for and prosecuting any criminal violation of law.

(2) CIVIL REDRESS.—Any plaintext or decryption information provided under this chapter to an investigative or law enforcement officer may not be disclosed, except by court order, to any other person for use in a civil proceeding that is unrelated to a criminal investigation and prosecution for which the plaintext or decryption information is authorized under paragraph (1). Such order shall only issue upon a showing by the party seeking disclosure that there is no alternative means of obtaining the plaintext, or decryption information, being sought and the court also finds that the interests of justice would not be served by nondisclosure.

(b) LIMITATION.—An investigative or law enforcement officer may not use decryption information obtained under this chapter to determine the plaintext of any data, including communications, unless it has obtained lawful authority to obtain such data, including communications, under other lawful authorities.

(c) RETURN OF DECRYPTION INFORMATION.—An attorney for the Government shall, upon the issuance of an order of a court of competent jurisdiction—

(1)(A) return any decryption information to the person responsible for providing it to an investigative or law enforcement officer pursuant to this chapter; or

(B) destroy such decryption information, if the court finds that the interests of justice or public safety require that such decryption information should not be returned to the provider; and

(2) within 10 days after execution of the court's order to return or destroy the decryption information—

(A) certify to the court that the decryption information has either been returned or destroyed consistent with the court's order; and

(B) if applicable, notify the provider of the decryption information of the destruction of such information.

(d) OTHER DISCLOSURE OF DECRYPTION INFORMATION.—Except as otherwise provided in section 2803, decryption information or the plaintext of otherwise encrypted data, including communications, shall not be disclosed by any person unless the disclosure is—

(1) to the person encrypting the data, including communications, or an authorized agent thereof;

(2) with the consent of the person encrypting the data, 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 decryption information, including determinations arising from

legal proceedings associated with the incapacity, death, or dissolution of any person; or

(5) otherwise permitted by law.

§ 2806. Identification of decryption information

(a) IDENTIFICATION.—To avoid inadvertent disclosure of decryption information, any person who provides decryption information to an investigative or law enforcement officer pursuant to this chapter shall specifically identify that part of the material that discloses decryption information as such.

(b) RESPONSIBILITY OF INVESTIGATIVE OR LAW ENFORCEMENT OFFICER.—The investigative or law enforcement officer receiving any decryption information under this chapter shall maintain such information in a facility and in a method so as to reasonably assure that inadvertent disclosure does not occur.

§ 2807. Definitions

The definitions set forth in section 101 of the Encryption for the National Interest Act shall apply to this chapter.

* * * * * * *

○