105TH CONGRESS } HOUSE OF REPRESENTATIVES { REPT. 105–108
1st Session } { Part 4

SECURITY AND FREEDOM THROUGH ENCRYPTION ("SAFE") ACT OF 1997

SEPTEMBER 16, 1997.—Ordered to be printed

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

REPORT

together with

ADDITIONAL VIEWS

[To accompany H.R. 695]

[Including cost estimate of the Congressional Budget Office]

The Permanent Select Committee on Intelligence, to whom was referred the bill (H.R. 695) 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 "Security and Freedom Through Encryption ('SAFE') Act of 1997".

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

43–400

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 and improve the export of encryption products developed and manufactured in the United States, and to preserve public safety and national security.

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

(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, 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 September 1, 1997.

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

(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) KEY RECOVERY AGENT.—The term "key recovery agent" means a person trusted by another person or persons to hold and maintain sufficient decryption information to allow for the immediate decryption of the encrypted data or communications of another person or persons for whom that information is held, and who holds and maintains that information as a business or governmental practice, whether or not for profit. The term "key recovery agent" includes any person who holds his or her decryption information.

(15) NATIONAL SECURITY.—The term "national security" means the national defense, foreign relations, or economic interests of the United States.

(16) PLAINTEXT.—The term "plaintext" means the readable or comprehensible format of data, including communications, prior to its being encrypted or after it has been decrypted.

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

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

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

(20) TELECOMMUNICATIONS CARRIER.—The term "telecommunications carrier" has the meaning given that term in section 102(8) of the Communications Assistance for Law Enforcement Act (47 U.S.C. 1001(8)).

(21) 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 other medium.

(22) 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 key length chosen, or implementation technique or medium used.

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

(a) USE IS VOLUNTARY.—The use of certificate authorities or key recovery agents is voluntary.

(b) REGULATIONS.—The Secretary shall promulgate regulations establishing standards for creating key management infrastructures. Such regulations should—

(1) allow for the voluntary participation by private persons and non-Federal entities; and

(2) promote the development of certificate authorities and key recovery agents.

(c) REGISTRATION OF CERTIFICATE AUTHORITIES AND KEY RECOVERY AGENTS.—Certificate authorities and key recovery agents meeting the standards established by the Secretary may be registered by the Secretary if they so choose, and may identify themselves as meeting the standards of the Secretary.

SEC. 104. UNLAWFUL USE OF ENCRYPTION.

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

"CHAPTER 122—ENCRYPTED 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 alone shall not constitute 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. Unlawful sale of encryption

"Whoever, after January 31, 2000, sells in interstate or foreign commerce any encryption product that does not include features or functions permitting duly authorized persons immediate access to plaintext or immediate decryption capabilities shall be imprisoned for not more than 5 years, fined under this title, or both.

"§ 2804. Encryption products manufactured and intended for use in the United States

"(a) PUBLIC NETWORK SERVICE PROVIDERS.—After January 31, 2000, public network service providers offering encryption products or encryption services shall ensure that such products or services enable the immediate decryption or access to plaintext of the data, including communications, encrypted by such products or services on the public network upon receipt of a court order or warrant, pursuant to section 2806.

"(b) MANUFACTURERS, DISTRIBUTORS, AND IMPORTERS.—After January 31, 2000, it shall be unlawful for any person to manufacture for distribution, distribute, or import encryption products intended for sale or use in the United States, unless that product—

"(1) includes features or functions that provide an immediate access to plaintext capability, through any means, mechanism, or technological method that—

"(A) permits immediate decryption of the encrypted data, including communications, upon the receipt of decryption information by an authorized party in possession of a facially valid order issued by a court of competent jurisdiction; and

"(B) allows the decryption of encrypted data, including communications, without the knowledge or cooperation of the person being investigated, subject to the requirements set forth in section 2806;

"(2) can be used only on systems or networks that include features or functions that provide an immediate access to plaintext capability, through any means, mechanism, or technological method that—

"(A) permits immediate decryption of the encrypted data, including communications, upon the receipt of decryption information by an authorized party in possession of a facially valid order issued by a court of competent jurisdiction; and

"(B) allows the decryption of encrypted data, including communications, without the knowledge or cooperation of the person being investigated, subject to the requirements set forth in section 2806; or

"(3) otherwise meets the technical requirements and functional criteria promulgated by the Attorney General under subsection (c).

"(c) ATTORNEY GENERAL CRITERIA.—

"(1) PUBLICATION OF REQUIREMENTS.—Within 180 days after the date of the enactment of this chapter, the Attorney General shall publish in the Federal Register technical requirements and functional criteria for complying with the decryption requirements set forth in this section.

"(2) PROCEDURES FOR ADVISORY OPINIONS.—Within 180 days after the date of the enactment of this chapter, the Attorney General shall promulgate procedures by which data network service providers and encryption product manufacturers, sellers, re-sellers, distributors, and importers may obtain advisory opinions as to whether an encryption product intended for sale or use in the United States after January 31, 2000, meets the requirements of this section and the technical requirements and functional criteria promulgated pursuant to paragraph (1).

"(3) PARTICULAR METHODOLOGY NOT REQUIRED.—Nothing in this chapter or any other provision of law shall be construed as requiring the implementation of any particular decryption methodology in order to satisfy the requirements of subsections (a) and (b), or the technical requirements and functional criteria required by the Attorney General under paragraph (1).

"(d) USE OF PRIOR PRODUCTS LAWFUL.—After January 31, 2000, it shall not be unlawful to use any encryption product purchased or in use prior to such date.

"§ 2805. Injunctive relief and proceedings

"(a) INJUNCTION.—Whenever it appears to the Secretary or the Attorney General that any person is engaged in, or is about to engage in, any act that constitutes, or would constitute, a violation of section 2804, the Attorney General may initiate a civil action in a district court of the United States to enjoin such violation. Upon the filing of the complaint seeking injunctive relief by the Attorney General, the court shall automatically issue a temporary restraining order against the party being sued.

"(b) BURDEN OF PROOF.—In a suit brought by the Attorney General under subsection (a), the burden shall be upon the Government to establish by a preponderance of the evidence that the encryption product involved does not comport with the requirements set forth by the Attorney General pursuant to section 2804 providing for immediate access to plaintext by Federal, State, or local authorities.

"(c) CLOSING OF PROCEEDINGS.—(1) Upon motion of the party against whom injunction is being sought—

"(A) any or all of the proceedings under this section shall be closed to the public; and

"(B) public disclosure of the proceedings shall be treated as contempt of court.

"(2) Upon a written finding by the court that public disclosure of information relevant to the prosecution of the injunction or relevant to a determination of the factual or legal issues raised in the case would cause irreparable or financial harm to the party against whom the suit is brought, or would otherwise disclose proprietary information of any party to the case, all proceedings shall be closed to members of the public, except the parties to the suit, and all transcripts, motions, and orders shall be placed under seal to protect their disclosure to the general public.

"(d) ADVISORY OPINION AS DEFENSE.—It is an absolute defense to a suit under this subsection that the party against whom suit is brought obtained an advisory opinion from the Attorney General pursuant to section 2804(c) and that the product at issue in the suit comports in every aspect with the requirements announced in such advisory opinion.

"(e) BASIS FOR PERMANENT INJUNCTION.—The court shall issue a permanent injunction against the distribution of, and any future manufacture of, the encryption product at issue in the suit filed under subsection (a) if the court finds by a preponderance of the evidence that the product does not meet the requirements set forth by the Attorney General pursuant to section 2804 providing for immediate access to plaintext by Federal, State, or local authorities.

"(f) APPEALS.—Either party may appeal, to the appellate court with jurisdiction of the case, any adverse ruling by the district court entered pursuant to this section. For the purposes of appeal, the parties shall be governed by the Federal Rules of Appellate Procedure, except that the Government shall file its notice of appeal not later than 30 days after the entry of the final order on the docket of the district court. The appeal of such matter shall be considered on an expedited basis and resolved as soon as practicable.

"§ 2806. Court order access to plaintext

"(a) COURT ORDER.—(1) A court of competent jurisdiction shall issue an order, ex parte, granting an investigative or law enforcement officer immediate 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 or foreign counterintelligence 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 or foreign counterintelligence 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 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) OTHER ORDERS.—An attorney for the Government may make application to a district court of the United States for an order under subsection (a), upon a request from a foreign country pursuant to a Mutual Legal Assistance Treaty with such country that is in effect at the time of the request from such country.

"(c) 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 shall 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.

"(d) 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.

"(e) 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 that would otherwise remain encrypted.

"§ 2807. 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 2806 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 that 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, have 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. On an ex parte showing of good cause to a court of competent jurisdiction, the serving of the inventory required by this subsection may be postponed.

"(b) ADMISSION INTO EVIDENCE.—The contents 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 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.

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

"(d) 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 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 unlawfully decrypted or accessed;

"(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.

"(e) 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 (d), or the denial of an application for an order under section 2806, if the United States attorney 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.

"(f) CIVIL ACTION FOR VIOLATION.—Except as otherwise provided in this chapter, any person described in subsection (g) 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.

"(g) COVERED PERSONS.—Subsection (f) 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.

"(h) LIMITATION.—A civil action under subsection (f) 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.

"(i) 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.

"(j) 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 a timely or reasonable fashion. The court, upon notice to the Government, shall decide such motion expeditiously.

"(k) 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.

"§ 2808. 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 use such plaintext or decryption information for the purposes of conducting a lawful criminal investigation or foreign counterintelligence 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 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) 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 2806, a key recovery agent may not disclose decryption information stored with the key recovery agent by a person unless the disclosure is—

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

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

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

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

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

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

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

"§ 2809. Identification of decryption information

"(a) IDENTIFICATION.—To avoid inadvertent disclosure, 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 provided 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 facilities and in a method so as to reasonably assure that inadvertent disclosure does not occur.

"§ 2810. Unlawful export of certain encryption products

"Whoever, after January 31, 2000, knowingly exports an encryption product that does not include features or functions providing duly authorized persons immediate access to plaintext or immediate decryption capabilities, as required under law, shall be imprisoned for not more than 5 years, fined under this title, or both.

"§ 2811. Definitions

"The definitions set forth in section 101 of the Security and Freedom through Encryption ('SAFE') Act of 1997 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:

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

TITLE II—GOVERNMENT PROCUREMENT

SEC. 201. FEDERAL PURCHASES OF ENCRYPTION PRODUCTS.

After January 1, 1999, any encryption product or service purchased or otherwise procured by the United States Government to provide the security service of data confidentiality for a Federal computer system shall include a technique enabling immediate decryption by an authorized party without the knowledge or cooperation of the person using such encryption products or services.

SEC. 202. ENCRYPTION PRODUCTS PURCHASED WITH FEDERAL FUNDS.

After January 1, 1999, any encryption product or service purchased directly with Federal funds to provide the security service of data confidentiality shall include a technique enabling immediate decryption by an authorized party without the knowledge or cooperation of the person using such encryption product or service unless the Secretary, with the concurrence of the Attorney General, determines implementing this requirement would not promote the purposes of this Act.

SEC. 203. NETWORKS ESTABLISHED WITH FEDERAL FUNDS.

After January 1, 1999, any communications network established with the use of Federal funds shall use encryption products which include techniques enabling immediate decryption by an authorized party without the knowledge or cooperation of

the person using such encryption products or services unless the Secretary, with the concurrence of the Attorney General, determines implementing this requirement would not promote the purposes of this Act.

SEC. 204. PRODUCT LABELS.

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

SEC. 205. NO PRIVATE MANDATE.

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

SEC. 206. IMPLEMENTATION.

(a) 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.

(b) RULEMAKING.—The Secretary, in consultation with the Attorney General and other affected agencies, may through rules provide for the orderly implementation of this title and the effective use of secure public networks.

TITLE III—EXPORTS OF ENCRYPTION

SEC. 301. EXPORTS OF ENCRYPTION.

(a) COORDINATION OF EXECUTIVE BRANCH AGENCIES REQUIRED.—The Secretary, in close coordination with the Secretary of Defense and any other executive branch department or agency with responsibility for protecting the national security, shall have the authority to control the export of encryption products not controlled on the United States Munitions List.

(b) DECISIONS NOT SUBJECT TO JUDICIAL REVIEW.—Decisions made by the Secretary pursuant to subsection (a) with respect to exports of encryption products under this title shall not be subject to judicial review.

SEC. 302. LICENSE EXCEPTION FOR CERTAIN ENCRYPTION PRODUCTS.

(a) LICENSE EXCEPTION.—After January 31, 2000, encryption products, without regard to encryption strength, shall be eligible for export under a license exception if such encryption product—

(1) is submitted to the Secretary for a 1-time product review;

(2) does not include features or functions that would otherwise require licensing under applicable regulations;

(3) is not destined for countries, end users, or end uses that the Secretary, in coordination with the Secretary of Defense and other executive branch departments or agencies with responsibility for protecting the national security, by regulation, has determined should be ineligible to receive such products, and is otherwise qualified for export; and

(4)(A) includes features or functions providing an immediate access to plaintext capability, if there is lawful authority for such immediate access; or

(B) includes features or functions providing an immediate decryption capability of the encrypted data, including communications, upon the receipt of decryption information by an authorized party, and such decryption can be accomplished without unauthorized disclosure.

(b) ENABLING OF DECRYPTION CAPABILITIES.—The features or functions described in subsection (a)(4) need not be enabled by the manufacturer before or at the time of export for purposes of this title. Such features or functions may be enabled by the purchaser or end user.

(c) RESPONSIBILITIES OF THE SECRETARY.—The Secretary, in close coordination with the Secretary of Defense and other executive branch departments or agencies with responsibility for protecting the national security, shall—

(1) specify, by regulation, the information that must be submitted for the 1-time review referred to in this section; and

(2) make all export determinations under this title within 30 days following the date of submission to the Secretary of—

(A) the completed application for a license exception; and

(B) the encryption product intended for export that is to be reviewed as required by this section.

(d) EXERCISE OF OTHER AUTHORITIES.—The Secretary, and the Secretary of Defense, 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 section.

(e) PRESUMPTION IN FAVOR OF EXPORTS.—There shall be a presumption in favor of export of encryption products under this title.

(f) WAIVER AUTHORITY.—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 in the interests of national security or public safety and security. The President shall submit a report to the relevant committees of the Congress not later than 15 days after such determination. The report shall include the factual basis upon which such determination was made. The report may be in classified format.

(g) RELEVANT COMMITTEES.—The relevant committees of the Congress described in subsection (f) are the Committee on International Relations, the Committee on the Judiciary, the Committee on National Security, the Permanent Select Committee on Intelligence of the House of Representatives, and the Committee on Foreign Relations, the Committee on the Judiciary, the Committee on Armed Services, and the Select Committee on Intelligence of the Senate.

SEC. 303. LICENSE EXCEPTION FOR TELECOMMUNICATIONS PRODUCTS.

After a 1-time review as described in section 302, the Secretary shall authorize for export under a license exception voice encryption products that do not contain decryption or access to plainvoice features or functions otherwise required in section 302, if the Secretary, after consultation with relevant executive branch departments or agencies, determines that—

(1) information recovery requirements for such exports would disadvantage United States exporters; and

(2) such exports under a license exception would not create a risk to the foreign policy, non-proliferation, or national security of the United States.

SEC. 304. REVIEW FOR CERTAIN INSTITUTIONS.

The Secretary, in consultation with other executive branch departments or agencies, shall establish a procedure for expedited review of export license applications involving encryption products for use by qualified banks, financial institutions, subsidiaries of companies owned or controlled by United States persons, or other users specifically authorized by the Secretary.

SEC. 305. 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 promote the export of encryption products manufactured in the United States;

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

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

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

(6) 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;

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

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

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

(c) MEMBERSHIP.—(1) The Board shall be composed of 13 members, as follows:

(A) The Secretary, or the Secretary's designee, who shall chair the Board.

(B) The Attorney General, or the Director of the Federal Bureau of Investigation, or a respective designee.

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

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

(E) The Special Assistant to the President for National Security Affairs, or his or her designee.

(F) Two private sector individuals, appointed by the President, who have expertise in consumer and privacy interests relating to or affected by information security technology.

(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.

(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) 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.

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 and is not authorized by court order to disclose such plaintext or decryption information.

SEC. 402. COMPLIANCE DEFENSE.

Compliance with the provisions of sections 2806, 2807, 2808, or 2809 of title 18, United States Code, as added by section 104(a) of this Act, or any regulations authorized thereunder, 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. REASONABLE CARE DEFENSE.

The participation by person in the key management infrastructure established by regulation for United States Government information security operations under section 103 shall be treated as evidence of reasonable care or due diligence in any proceeding where the reasonableness of one's actions is an element of the claim at issue.

SEC. 404. GOOD FAITH DEFENSE.

An objectively reasonable reliance on the legal authority provided by this Act and the amendments made by this Act, requiring or authorizing access to the plaintext of otherwise encrypted data, including communications, or to the decryption information that will allow the immediate decryption of data, including communications, that is otherwise encrypted, shall be a complete defense to any criminal or civil action that may be brought under the laws of the United States or any State.

SEC. 405. SOVEREIGN IMMUNITY.

Except as otherwise specifically provided otherwise, nothing in this Act or the amendments made by this Act, or any regulations promulgated thereunder, modifies or amends the sovereign immunity of the United States.

SEC. 406. CIVIL ACTION, GENERALLY.

A civil action may be brought against any person who, regardless of that person's participation in the key management infrastructure to be established by regulations promulgated by the Secretary pursuant to section 103, violates or acts in a manner that is inconsistent with or violates the provisions or intent of this Act or the amendments made by this Act.

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 mutual recognition of any key management infrastructures, and their component parts, that exist or are developed; and

(2) such mutual recognition agreements will 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 mutual recognition 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 December 15, 1998.

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 the instances in which encryption has interfered with, impeded, or obstructed the ability of the Department of Justice to enforce the criminal laws of the United States.

(b) AVAILABILITY OF INFORMATION TO THE CONGRESS.—The information compiled under subsection (a), including an unclassified summary thereof, shall be made available, upon request, to any Member of Congress.

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. 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

Americans expect their phone calls, electronic mail, personal documents, and electronic commercial activities to be secure and pri-

vate. The rapid expansion of communication and computer technology has created vulnerabilities that leave many personal communications and commercial transactions potentially exposed to fraud and misuse. The development and use of strong encryption is essential to a thriving electronic communications capability, and necessary to help safeguard privacy and protect ourselves from crime. H.R. 695 promotes the development and distribution of strong encryption technologies that are intended to provide a heightened level of security and freedom to engage in electronic commerce.

Chief among the government's obligations to its people is the duty to protect them from threats of harm to their persons or property. Similarly, in order to establish and maintain a government that serves the common good and provides for the common defense, which the Framers acknowledged was essential to a free society, national security interests must be carefully weighed against the people's inalienable rights of life, liberty, and property. With this interest in maintaining the balance between individual rights and our nation's security, the Permanent Select Committee on Intelligence sought and obtained referral of the bill, H.R. 695. The Committee's consideration of H.R. 695 brought to light that the bill as introduced and reported by the Committee on the Judiciary, though certainly well-intentioned, left our intelligence and intelligence-related capabilities at considerable risk. Likewise, enacted without amendment, it might jeopardize the nation's (including our state and local law enforcement agencies) ability to investigate, apprehend, and prosecute criminals of the most serious stripe.

The Committee received evidence that strong encryption has already been used to facilitate drug trafficking, protect child pornographers, shield terrorist plots and communications, and hide evidence of credit card fraud, among other notable crimes. Furthermore, the Committee is of the view that such a law enforcement and national security risk should not be left to the forces of the marketplace. Doing so abdicates the responsibility of the government to protect its people from enemies, both foreign and domestic.

Thus, the amendment in the nature of a substitute to H.R. 695, reported favorably by the Committee, seeks simply to ensure that the critical national security and law enforcement concerns at issue in this debate over the nature and direction of encryption policy for the United States will be seriously addressed.

SUMMARY

SECTION-BY-SECTION

Section 1.—Short title

This section provides the title of the bill as the "Security and Freedom through Encryption ("SAFE") Act of 1997."

Section 2.—Statement of policy

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

TITLE I—DOMESTIC USES 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.—Voluntary private sector participation in key management infrastructure

Subsection (a) clarifies that the use of certificate authorities or key recovery agents is completely voluntary.

Subsection (b) provides the Secretary of Commerce with regulatory authority to establish standards for creating voluntary key management infrastructures. The Committee believes that the development of key management infrastructures is important to the interoperability that is necessary for the further development of safe and secure electronic commerce. Any regulations promulgated should allow the voluntary participation of private persons and non-federal entities. These regulations should also encourage the development of certificate authorities and key recovery agents.

Subsection (c) will permit key recovery agents or certificate authorities to register themselves with the Commerce Department. In addition, such entities will be allowed, if they choose, to identify themselves as meeting the standards established by the Secretary.

Section 104.—Unlawful use of encryption

This section amends Title 18, United States Code, by new sections 2801 through 2811 within a 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, the potential penalties are not more than 5 years in prison, a fine under Title 18, United States Code,[1] or both. For repeat offenders of this provision, the jail time is potentially no more than an additional 10 years. This section would apply equally to any investigative or law enforcement officer who is found to have violated these provisions.

New section 2801 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. Next, it makes it a criminal offense to exceed lawful authority in

[1] Title 18, United States Code, Section 3571 establishes the fine schedule for all Title 18 criminal violations. For an individual convicted of a felony, the fine would, generally, be $250,000. For an organization convicted of a felony, the fine would, generally, be $500,000. Some specific criminal provisions may specify higher fine amounts. Any criminal provision authorizing a lower fine amount is nullified by enactment of subsection (e) of section 3571 of Title 18, United States Code.

decrypting data, including communications. This new section would make the breaking of the 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. Likewise, it would be illegal to impersonate another for the purpose of obtaining that person's decryption information without lawful authority. Importantly, it also makes it unlawful to facilitate or assist in the encryption of data, including communications, that are to be used in furtherance of a crime. Finally, it makes it illegal to otherwise disclose decryption information in violation of the provisions of new chapter 122 of Title 18, United States Code. Each of these criminal violations is subject to a potential penalty of not more than 10 years in prison, a fine under Title 18, United States Code, or both. This section would apply equally to any investigative or law enforcement officer who is found to have violated these provisions.

New section 2803 will make it unlawful after January 31, 2000, to sell in interstate or foreign commerce any encryption product that does not provide duly authorized persons an immediate access to plaintext capability, or immediate decryption capability. Under this new chapter of Title 18, United States Code, such duly authorized persons only include those presenting an order from a court of competent jurisdiction requiring that such access or provision of decryption information be made. This section would apply equally to any investigative or law enforcement officer who is found to have violated these provisions.

New section 2804 establishes manufacturing and service requirements on encryption products intended for distribution and use after January 31, 2000. Subsection (a) requires all public network service providers to offer encryption products or services that ensure an immediate decryption capability or an immediate access to plaintext capability.

Subsection (b) requires any person who manufactures for distribution, distributes, or imports encryption products intended for sale or use in the United States to include in such products features or functions that provide an immediate access to plaintext capability. These features or functions must permit the immediate decryption of data, including communications, without the knowledge or cooperation of the person being investigated, but only upon the presentation of a facially valid order issued by a court of competent jurisdiction. Alternatively, encryption products may be manufactured for distribution, distributed, or imported even if they do not meet the requirements set forth above, so long as they can be used only on systems or networks that include features or functions that otherwise provide the immediate access to plaintext capability previously discussed. Finally, persons are free to manufacture encryption products that do not comport with any of the requirements set forth here, so long as they otherwise meet the technical requirements and functional criteria established by the Attorney General, pursuant to subsection (c).

Subsection (c) provides the Attorney General with regulatory authority to promulgate technical requirements and functional criteria for encryption products that will allow for an immediate access to plaintext capability, or otherwise enable the immediate

decryption of the otherwise encrypted data, including communications. This subsection provides industry with an opportunity to seek an advisory opinion from the Attorney General as to a particular product intended for manufacturer or distribution. Such advisory opinions serve an important function in that they will provide the industry with clear guidance on products intended for sale. This procedure will hopefully alleviate the need for lawsuits to enjoin the distribution or manufacture of encryption products. This subsection specifically provides that the Attorney General cannot require a particular methodology to be used in meeting her technical requirements or functional criteria.

Subsection (d) authorizes the use, even after January 31, 2000, of encryption products purchased or in use prior to that date. This alleviates any ex post facto problem. The Committee also recognizes that industry will need to develop new product lines to comply with the provisions of this amendment. Thus, in order to allow those manufacturers an opportunity to recoup some of their research and development investment this provision allows them to continue to sell their current product line for the next two-plus years.

New section 2805 sets forth procedures whereby the onus is on the government to prohibit the manufacture or distribution of an encryption product, after January 31, 2000, that she or the Secretary of Commerce believes does not meet the technical requirements or functional criteria established by the Attorney General. The Committee believes that it is appropriate for the Attorney General to bear the burden, in a court of law, before an independent arbiter of the facts, of keeping a particular encryption product out of the market place. The provision allows for the closure of such proceedings to protect the proprietary interest in any information that might be disclosed through a public proceeding. Furthermore, the provision will provide those who obtained an advisory opinion with an absolute defense to the lawsuit as long as the product at issue comports in every aspect with the requirements announced in the Attorney General's advisory opinion.

New section 2806 sets forth the standards and procedures for the issuance of a court order granting an investigative or law enforcement officer access to the plaintext of otherwise encrypted data, including communications, or compelling the provision of decryption information to an investigative or law enforcement officer. 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 or decryption information is relevant to an on-going and legitimate law enforcement or foreign counterintelligence investigation. The application and any order issued thereon may be made ex parte and placed under seal. Disclosure of the application or order is not authorized by anyone, except as otherwise permitted by this section, or another order of the court. This section also comports with any obligation the United States may have to any foreign government under any effective Mutual Legal Assistance Treaties

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

decryption information be maintained. This record shall not be maintained in a place or in a manner under the custody or control of the investigative or law enforcement officer gaining the access under this section. The record will then 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 of data, including communications, for which it previously obtained lawful authority to intercept or obtain.

New section 2807 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 does provide for a delayed notification to the user so as not to jeopardize the integrity of the on-going criminal investigation or foreign counter-intelligence 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 the delay. Specifically, however, none 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 2808 limits the lawful uses of any plaintext or decryption information may be put. It may be used for the purposes of conducting a lawful criminal or foreign counterintelligence 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 the 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 the 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 to whom and under what circumstances decryption information may be provided to another person by a key recovery agent.

New section 2809 requires those who are providing decryption information to an investigative or law enforcement officer to so iden-

tify that information in order to avoid any inadvertent disclosure. The officer is responsible for maintaining the decryption information in such a manner so as to reasonably assure against inadvertent disclosure.

New section 2810 makes it a crime to knowingly export an encryption product after January 31, 2000 that does not include an immediate access to plaintext capability, or that does not provide an immediate decryption capability. This criminal provision carries a potential prison term of not more than 5 years.

New section 2811 incorporates the definitions set forth at section 101 of this Act as the definitions to be utilized for new chapter 122 of Title 18, United States Code.

TITLE II—GOVERNMENT PROCUREMENT

Section 201.—Federal purchases of encryption products

This section requires the United States Government, after January 1, 1999, to purchase only those encryption products enabling the immediate 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 obtained for providing security service for a federal computer system.

Section 202.—Encryption products purchased with Federal funds

This section requires that any encryption product or service purchased directly with federal funds after January 1, 1999, shall enable the immediate decryption by an authorized party, without the knowledge or cooperation of the person using the encryption product. The Committee does not intend that this provision applies to any product purchased by institutions receiving federal grants or other funding, if such institution does not require interoperability with the United States government, such as universities or public libraries.

Section 203.—Networks established with Federal funds

This section requires that any communications network that is established directly with federal funds after January 1, 1999, must use encryption products that include techniques enabling the immediate 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 satisfy this requirement. Rather, the Committee intends that this provision apply solely to those communication networks established for the purpose of communication with the United States government, either on a contractual basis, or as an element of the government.

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 articulates the policy that the United States government shall not require the use of particular encryption standards for the private sector.

Section 206.—Implementation

This section specifically states that encryption products used solely for access control, authentication, integrity, nonrepudiation, or digital signatures are not covered by the provisions of this title. Moreover, this section grants the Secretary of Commerce regulatory authority to effectuate the provisions of this title.

TITLE III—EXPORTS OF ENCRYPTION

Section 301.—Exports of encryption

Subsection (a) establishes that the Secretary of Commerce, acting in close coordination with the Secretary of Defense, and other executive branch agencies with responsibility for protecting the national security, has the authority to exercise control over the export of encryption products.

Subsection (b) clarifies that export control decisions made by the Secretary are not subject to judicial review.

Section 302.—License exception for certain encryption products

Subsection (a) sets criteria for export license exceptions of encryption products after January 31, 2000. Specifically, products eligible for exemptions must: be submitted to the Secretary of Commerce for a 1-time product review; not include features that would require licensing under other applicable regulations; not be destined for countries that are determined ineligible on national security grounds. In addition, the product must include a means of obtaining immediate access to plaintext capability if there is lawful authority for such access.

Subsection (b) clarifies that the immediate access to plaintext capability need not be enabled by the manufacturer before or at the time of export.

Subsection (c) requires the Secretary, in close coordination with the Secretary of Defense and other relevant executive branch agency heads, to promulgate regulations for the 1-time review process; and sets a time limit of 30 days for that review process. This subsection establishes that the 30-day time clock starts when the Secretary has received a completed application for license exception and the encryption product intended for export.

Subsection (d) clarifies that the Secretary of Commerce and the Secretary of Defense still maintain any authorities they currently possess under any other provisions of law, including the Export Administration Act of 1979, as continued in effect under the International Emergency Economic Powers Act.

Subsection (e) establishes a presumption in favor of exporting products submitted to the Secretary under this section. The burden will be on the Secretary of Commerce to deny export.

Subsection (f) provides the President with the authority to waive any portion 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.

Subsection (g) lists the committees in the House and Senate that would receive a report under the previous subsection.

Section 303.—License exception for telecommunications products

This section provides a specific exemption for certain voice encryption products. Products will be eligible for this exemption if, after a 1-time review, the Secretary of Commerce determines that the inclusion of information recovery capability would disadvantage U.S. exporters; and the export of the voice encryption product would not pose a risk to foreign policy, nonproliferation, or national security.

Section 304.—Review for certain institutions

This section requires the Secretary of Commerce to establish an expedited export license exception review process for encryption products to be used by qualified banks, financial institutions, U.S. businesses, and other users specifically authorized by the Secretary.

Section 305.—Encryption Industry and Information Security Board

This section establishes an Encryption Industry and Information Security Board ("EIISB") to advise the President on future encryption policy and technological advancements that would 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 13 members, and how those members shall be appointed. In addition to the Secretaries of Commerce and Defense, the Attorney General or the FBI Director, the Director of Central Intelligence, and the National Security Advisor to the President, or their designees will sit on the EIIS Board. The board shall include two individuals appointed by the President who should have no ties to the industry, but who can represent the interests of consumer groups and civil liberties advocacy groups. There will also be appointed six representatives from the private sector who together have expertise in the many facets of information security, including the technical and legal issues surrounding the use of information security technology. The Board will report to the President and Congress, and their recommendations are not binding.

TITLE IV—LIABILITY LIMITATIONS

Section 401.—Compliance with court order

This section states that a person shall not be held civilly or criminally liable 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 2806, 2807,

2808, or 2809 of title 18, United States Code, as added by section 104(a) of this Act, or any regulations authorized thereunder.

Section 403.—Reasonable care defense

This provision encourages the participation in a key management infrastructure that meets the standards suggested by the Secretary of Commerce under section 103 of this Act. This section authorizes the use of one's participation in such key management infrastructure as evidence of reasonable care in a case where the reasonableness of one's actions is at issue.

Section 404.—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, with a complete defense to any criminal or civil action arising therefrom.

Section 405.—Sovereign immunity

This section clarifies that nothing in this Act modifies or amends the sovereign immunity of the United States.

Section 406.—Civil action, generally

This section allows a civil action to be brought against any person who violates or acts in a way that is inconsistent with the provisions or intent of this Act.

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 mutual recognition of key management infrastructures.

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 December 15, 1998.

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 Economic Powers Act; it does not affect foreign intelligence activities of the United States; nor does it diminish US or State intellectual property protections.

Section 603.—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

H.R. 695, as amended by the Committee on the Judiciary, has broad implications on the intelligence and intelligence-related activities of the United States. The Intelligence Committee has jurisdiction over legislation relating to the intelligence and intelligence-related capabilities of the United States, including the FBI's domestic counter-intelligence and counter-terrorism functions. Thus, upon the Chairman's request, the Speaker referred the bill to the Committee for its consideration.

Primary among the Committee's concerns was how the development of strong and unbreakable encryption technology would affect the national security of the United States. The Defense Department's need for information security technology is essential to its force protection and war fighting functions. Likewise, information security is critical to the President and his advisors. It is necessary to the Department of State in its development of sound foreign policy. Encryption technology that does not provide for access points to plaintext, or the re-capture of communications and data, puts these needs at considerable risk.

The development of encryption technologies that does not take into consideration society's desire to prevent, investigate, and prosecute crimes, is of no sizable benefit to society. Such encryption technology would allow criminals to act with impunity, without concern that their actions might be subject to exposure by lawful authorities. The FBI, the agency primarily responsible for counter-terrorism and domestic counter-espionage efforts, and the investigation of child pornography and kidnapping, could find itself especially handicapped in these areas. Likewise, the Drug Enforcement Administration, which is responsible to the nation for counter-narcotics operations, could be negatively affected by H.R. 695. Similarly, the Committee was greatly concerned that State and local law enforcement agencies' ability to provide their citizenry with a free and peaceful place to live and work would be seriously jeopardized.

As considered by the Permanent Select Committee on Intelligence, H.R. 695 left the public's safety and our nation's security to the forces of the marketplace. The "SAFE" Act provided no mechanism or technological capability for law enforcement or national security to access the plaintext of data, including commu-

nications. It would ultimately have rendered meaningless any other law, including the Fourth Amendment, entitling law enforcement to such evidence. It would have negated our intelligence collectors' abilities to perform their vital national security functions. The Committee found that, to the detriment of the national security and law enforcement equities of the United States, H.R. 695 encouraged the development of unbreakable encryption technologies, seeming based upon an absolutist's view of the First Amendment and one's "right of privacy."

H.R. 695 did nothing to encourage the development of systems or software that would meet the crucial needs of national security or law enforcement. The bill placed the determination of whether a particular export of encryption technology affected the national security interests of the United States solely in the hands of the Secretary of Commerce, with no role whatsoever for the national security apparatus of the United States government. This, despite the proponents acknowledgment of the national security benefit that encryption technology can provide to the government.

The proponents of H.R. 695 argue that the legislation enhances the needs of law enforcement. They contend that strong encryption software, widely available to the public, will secure our computer networks, defeat fraud, and instill trust in the already booming Internet. This trust, they assert, is necessary to release the opportunities available through electronic commerce.

None of this is disputed.

Congress has on many occasions accepted the premise that the use of electronic surveillance is a tool of utmost importance in many criminal investigations, especially those involving serious and violent crime, terrorism, espionage, organized crime, drug-trafficking, corruption, and fraud. There have been numerous cases where law enforcement, through the use of electronic surveillance, has not only solved and successfully prosecuted serious crimes and dangerous criminals, but has also been able to prevent serious and life-threatening criminal acts. For example, terrorists in New York were plotting to bomb the United Nations building, the Lincoln and Holland tunnels, and 26 Federal Plaza as well as conduct assassinations of political figures. Court-authorized electronic surveillance enabled the FBI to disrupt the plot as explosives were being mixed. Ultimately, the evidence obtained was used to convict the conspirators. In another example, electronic surveillance was used to prevent and then convict two men who intended to kidnap, molest and then kill a male child.

The supporters of the bill insist that the problem for law enforcement is a narrow problem, only affecting approximately 1,100 wiretaps per year, while encryption provides great security benefits to the electronic marketplace.[2] The Committee is concerned that the problems posed by H.R. 695 are not as narrow as the bill's supporters claim. The problem that some see as "narrow" is in fact the entirety of the problem. Were the 1,100 or so wiretaps conducted by federal, state, and local law enforcement agencies across the country in the last year protected with unbreakable encryption, the

[2]Mr. Jerry Berman, Executive Director of the Center for Technology and Democracy before the House Judiciary Committee, March 20, 1997.

scores of drug traffickers, child pornographers, kidnappers, Mafiosi, terrorists, and spies that were identified, investigated, and prosecuted, through the use of those wiretaps, would still be at large.

The Committee notes, with considerable concern, that the threat such encryption creates is not limited to the FBI alone.

From a national security perspective, this is not a problem that will begin sometime in the future; we are already encountering the effects of encryption today. For example:

Convicted spy Aldrich Ames was told by the Russian intelligence service to encrypt computer file information that was to be passed to them;

An international terrorist was plotting to blow up 11 U.S.-owned commercial airliners in the far east. His laptop computer which was seized during his arrest in Manila contained encrypted files concerning this terrorist plot; and

A major international drug trafficking subject recently used a telephone encryption device to frustrate court-approved electronic surveillance.

H.R. 695 did little to facilitate or promote technological development of access points for interception, or provide for an immediate decryption capability, through a court order process. The Committee is of the view that these requirements can be fashioned in a way that does not undermine a citizen's right against unreasonable searches and seizures or unnecessarily abridge his or her freedom of speech. There is considerable precedent in statute for a regime that balances privacy, law enforcement concerns, and national security.[3]

The benefit that strong encryption, without access to plaintext capabilities, provides to the individual encryption user is equally provided to the person with criminal intent. The child pornographer will be able to operate with impunity. If there is no mechanism, no technological way of decrypting his files without his permission, there will be no way for the law to break his code, to access his computer files, to develop evidence of his criminal acts and bring him to justice. This is the world without a statutory requirement for access to plaintext capability for stored data, or communications.

---

[3]Title III of the Omnibus Crime Control Act of 1968 codified the government's authority to require service providers to supply technical assistance to enable law enforcement (Federal, state, and local) to intercept oral, electronic, and wire communications, upon the presentment of a court order. That Act balanced the competing rights of the individual and the government under the 4th Amendment by setting out in the statute judicial oversight, minimization, and delayed notification procedures that have met the test of time. That Act established the constitutionality of a government mandate upon technology for the societal benefit of public safety and national security.

The Communications Assistance to Law Enforcement Act ("CALEA"), building on the wiretap statutes, and considering the advancement of digital telecommunications capabilities, specifically required telecommunications common carriers to provide technical assistance and to develop software that will enable the government to maintain its capability to intercept communications, where otherwise allowable under the law. Furthermore, CALEA established the precedent that telecommunications companies that provide digital telephony to their customers must provide law enforcement with an access point to such communications so that the conversations occurring over such digital telecommunication devices are comprehensible.

The Committee also considered those statutes governing pen registers and trap and trace devices (18 U.S.C. sec. 3121–27), the use of classified information in the prosecution of criminal violations of federal law (18 U.S.C. App. 3, sec. 1, et seq.), and considered the practice of law enforcement in gaining access to bank records and other records held by third parties. The Committee also reviewed the fine balancing of interests that is manifest in the Foreign Intelligence Surveillance Act, 50 U.S.C.

Likewise, without access to plaintext capability for our intelligence collectors, international terrorists communicating across the Internet, or through digital communications, sending encrypted messages to their comrades discussing their plans to attack United States interests, can rest assured that their conspiracy will not be discovered, penetrated, frustrated, nor prosecuted by law enforcement authorities.

To be sure, as envisioned by the authors of the Bill of Rights, the Fourth Amendment stands as a bulwark against unreasonable government intrusion into the lives of its citizens. That freedom is jealously guarded by the people, through the power and authority of the Judicial Branch of our governmental structure. Certainly, the use of encryption technology to protect electronic data and communication accesses the same right to privacy as the use of a safe to protect paper documents.

Nothing in our constitutional framework, however, provides for absolutes. There is no absolute freedom of expression. There is no absolute freedom from search and seizure. Nothing about computer technology alters this constitutional truism. The Bill of Rights delicately balances the competing interests of the people and the nation. The Constitution recognizes that the freedoms embodied in the Bill of Rights are joined with responsibilities. The people are responsible for acting within the bounds of the law. The government, on the other hand, is responsible for acting reasonably. When a citizen violates the law, the Constitution permits reasonable government action to discover and expose that criminal activity. This is the essence of the Fourth Amendment. The Committee notes with concern that encryption technology, which will have enormous benefits, can also threaten the underpinnings of the Constitutional balance struck in the text of the Fourth Amendment if the technology is allowed to develop unchecked and without regard to one's civic responsibilities.

The privacy interests of encryption users should not be minimized, nor given absolute value. A balance must be established. It is true that access to decryption information could give the government an opportunity for mischief. Statutory safeguards against the impermissible use of decryption information can be employed to adequately deter such violations of privacy. Additionally, users of encryption should be notified that their decryption information has been accessed. But, the timing of this notification, like that permitted by the wiretap statute, is very important to the integrity of any criminal or counter-intelligence investigation.

With respect to export controls over encryption products, including software, hardware, and technology, it is important to the country's security interests to permit the export only of those encryption products that fulfill the goals of promoting and securing information systems of American citizens, while at the same time enabling the intelligence community to continue to support our policy makers, deployed forces, and U.S. interests at home and overseas.

Currently, the Administration regulates the export of encryption products and requires a license prior to export. On October 1, 1996, the Vice President announced for the Administration that it would begin allowing 56-bit DES encryption products, or its equivalent, under a general license upon the presentment of the product for a

one-time review so long as the exporting company committed to building and marketing future products that were supportive of key recovery. On November 1, 1996, President Clinton issued Executive Order 13026, 61 Fed. Reg. 58767 (November 19, 1996) implementing the policy outlined by the Vice President the month before. The Administration, through Ambassador Aaron, the U.S. Special Envoy for Encryption Policy, is also currently engaged in a multilateral effort to reach agreement in the international community on export standards supportive of key recovery products.

Proponents of H.R. 695 argue that export barriers need to be removed to enhance and improve the already superior position of American encryption manufacturers in foreign markets. They contend that our software industry will in a matter of years, under the current regulatory regime, suffer substantial losses in terms of jobs and profits. They argue that there are encryption products already widely available in foreign countries and on the Internet that are competing with U.S. manufactured encryption products and in the near term could strip U.S. industry of its preeminence in this field.

Foreign availability is an issue that is repeatedly raised in the encryption debate. Industry claims that encryption products are widely available overseas, that other countries do not control their export, and that American firms are suffering significant losses. A study of this issue found that claims of widespread foreign availability of encryption products were not entirely accurate. According to industry experts, widespread use of foreign encryption has not become manifest, although the pace of change and the market for information technology is rapid and a growing number of strong encryption products exist.

Only a few countries, other than the United States, produce encryption products at this time. Some, like Switzerland, produce only specialized products for a small segment of the market. Others, like Japan, produce primarily hardware products. These countries all have export controls on encryption. As noted, Ambassador Aaron is engaged in regular discussions with them. The Committee believes that the issue of foreign availability is one which the Administration must closely monitor as we move toward a permanent policy on encryption.

The Committee shares the concern that American encryption products could be replaced by foreign competitors. It notes, however, that the American grip on the market is remarkable, not just for its share of the market, but for its longevity. American technology manufacturers control no less than 75% of the global market, despite what many consider to be a "restrictive" policy on encryption products. It is acknowledged on both sides of this issue that American encryption technology is the best in the world. There is no desire to undermine that position, nor diminish the U.S. preeminence in this regard.

CONCLUSION

The encryption policy of the United States requires a comprehensive approach that takes into account the equities and prerogatives of the intelligence community; 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 the bill as re-

ported by the Committee on the Judiciary, which is further explained in the section-by-section analysis, makes an effort at balancing the important national security, public safety, and privacy interests that are at stake in this debate.

COMMITTEE PROCEEDINGS

The Committee was briefed on the subject of encryption on May 6, 1997 by the Hon. William Reinsch, Under Secretary, Bureau of Export Administration, Department of Commerce; Hon. William Crowell, Deputy Director, National Security Agency; and Hon. Robert Litt, Deputy Assistant Attorney General, Criminal Division, United States Department of Justice.

The Committee held a hearing on September 9, 1997 in which it heard testimony from: the Hon. Bob Goodlatte, United States Representative, 6th District of Virginia; Hon. Zoe Lofgren, United States Representative, 16th District of California; Hon. Louis J. Freeh, Director, Federal Bureau of Investigation; Hon. William Reinsch, Under Secretary, Bureau of Export Administration, Department of Commerce; and Hon. William Crowell, Deputy Director, National Security Agency.

The Committee extensively reviewed additional testimony and written materials relating to encryption policy in general and H.R. 695 in particular, including: "Terrorism in the Next Millennium: Enter the Cyberterrorist," by George R. Barth, National Counterintelligence Center; "Deciphering the Cryptography Debate," by Kenneth Flamm, The Brookings Institution; Hon. Michelle Van Cleave, Assistant Director for National Security, White House Office of Science and Technology Policy, remarks before AFCEA Convention, June 25, 1992; Hon. Janet Reno, United States Attorney General, letter to Members of Congress, July 18, 1997; Hon. Louis J. Freeh, Director, Federal Bureau of Investigation, testimony before the United States Senate Committee on Commerce, Science and Transportation, March 19, 1997; Hon. Louis J. Freeh, testimony before the United States Senate Committee on the Judiciary, June 25, 1997; Hon. John Kyl, United States Senator, Arizona, remarks before the Heritage Foundation, July 28, 1997;

Testimony before the United States Senate Judiciary Subcommittee on Technology, Terrorism and Government Information, September 3, 1997: Hon. Louis J. Freeh, Director, Federal Bureau of Investigation; Dorothy E. Denning, Georgetown University; Jeffery A. Herig, Special Agent, Florida Department of Law Enforcement; Robert R. Burke, Director of Corporate Services and Security, Monsanto Company, and Chairman of the Subcommittee for Protection of Information and Technology, Overseas Security Advisory Council, United States Department of State; Ken Lieberman, Senior Vice President for Corporate Risk Management, Visa USA; R. Patrick Watson, Director, Worldwide Corporate Security, Eastman Kodak Company;

Testimony before the United States House of Representatives Commerce Subcommittee on Telecommunications, Trade, and Consumer Protection, September 4, 1997: Hon. Bob Goodlatte, United States Representative, 6th District of Virginia; Hon. William Reinsch, Under Secretary, Bureau of Export Administration, Department of Commerce; Hon. Robert Litt, Deputy Assistant At-

torney General, Criminal Division, Department of Justice; Stephen T. Walker, President and CEO, Trusted Information Systems, Inc.; Thomas Parenty, Director of Data/Communications Security, Sybase, Inc.; George A. Keyworth, II, Ph.D., Chairman, Progress & Freedom Foundation; Jerry Berman, Executive Director, Center for Democracy and Technology;

Hearing records of: Hearing on H.R. 3011 (104th Congress), before the United States House of Representatives Committee on the Judiciary, September 25, 1996; Hearing on H.R. 695, before the United States House of Representatives Judiciary Subcommittee on Courts and Intellectual Property, March 20, 1997; and the redacted released transcript of the United States House of Representatives International Relations Committee Members' briefing, June 26, 1997.

In addition, the Committee staff was briefed on the subject of encryption from representatives of IBM, ORACLE, Center for Technology and Democracy, Netscape, and Motorola.

COMMITTEE CONSIDERATION

The Committee met on September 11, 1997, and in open session approved, by voice vote, the Goss/Dicks amendment in the nature of a substitute to H.R. 695, as amended and reported by the Committee on the Judiciary. The Committee, in open session, ordered H.R. 695, as amended, reported favorably by voice vote, a quorum being present.

VOTE OF THE COMMITTEE

During its consideration of H.R. 695, the Committee took no roll-call votes.

FINDINGS AND RECOMMENDATIONS OF THE COMMITTEE ON GOVERNMENT REFORM AND OVERSIGHT

With respect to clause 2(l)(3)(D) of rule XI of the Rules of the House of Representatives, the Committee has not received a report form the Committee on Government Reform and Oversight pertaining to the subject of the bill.

OVERSIGHT FINDINGS

In compliance with clause 2(l)(3)(A) of rule XI of the Rules of the House of Representatives, the Committee reports that the findings and recommendations of the Committee, based on oversight activities under clause 2(b)(1) of rule X of the Rules of the House of Representatives, are incorporated in the descriptive portions of this report.

NEW BUDGET AUTHORITY AND TAX EXPENDITURES

Clause 2(l)(3)(B) of House rule XI does not apply because this legislation does not provide new budgetary authority or increased tax expenditures.

CONGRESSIONAL BUDGET OFFICE ESTIMATES

U.S. CONGRESS,
CONGRESSIONAL BUDGET OFFICE,
Washington, DC, September 16, 1997.

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. 695, the Security and Freedom Through Encryption (SAFE) Act.

If you wish further details on this estimate, we will be pleased to provide them. The CBO staff contacts are Rachel Forward (for federal costs); Alyssa Trzeszkowski (for revenues); Pepper Santalucia (for the state and local impact); and Jean Wooster (for the private-sector impact).

Sincerely,

JAMES L. BLUM
(For June E. O'Neill, *Director*).

Enclosure.

H.R. 695—Security and Freedom Through Encryption (SAFE) Act of 1997

Summary: H.R. 695 would establish policies for the domestic use and export of encryption products that facilitate the creation of secure computer networks.

Assuming appropriation of the necessary amounts, CBO estimates that enacting this bill would result in additional discretionary spending of between $4.5 million and $7.1 million over the 1998–2002 period by the Bureau of Export Administration (BXA) and the Department of Justice (DOJ). Spending by BXA and DOJ for activities required by H.R. 695 would total between $9 million and $11.6 million over the next five years—as compared to spending by BXA of about $4.5 million over the same period under current policies. (Spending related to monitor encryption products by DOJ is negligible under current law.)

Enacting H.R. 695 also would affect direct spending and receipts beginning in fiscal year 1998 through the imposition of criminal fines and the resulting spending from the Crime Victims Fund. Therefore, pay-as-you-go procedures would apply. CBO estimates, however, that the amounts of direct spending or receipts would not be significant.

H.R. 695 contains an intergovernmental mandate as defined in the Unfunded Mandates Reform Act (UMRA), but CBO cannot estimate the cost of complying with that mandate at this time. The bill also would impose a private-sector mandate on public network service providers and manufacturers, distributors, and importers of encryption products. CBO estimates that the total direct cost of complying with this mandate would exceed the statutory threshold ($100 million in 1996, adjusted annually for inflation) for private-sector mandates established in UMRA. CBO's full analysis of the cost of the intergovernmental and the private-sector mandates will be provided under separate cover.

Description of the bill's major provisions: H.R. 695 would establish controls for the domestic use and export of encryption technologies. The bill would allow individuals in the United States to use any form of encryption but would prevent the sale of encryption products without plaintext recovery systems after January 31, 2000. (The term "plaintext" means the readable or comprehensible format of information.) The bill would authorize the Department of Commerce to exempt encryption products with plaintext recovery systems from certain export licensing requirements after the same date. In addition, H.R. 695 would require the Secretary of Commerce to establish a key management system for use by the federal government and private-sector organizations. A key management system enables agencies or companies to entrust the code to encryption products to a third party.

H.R. 695 would establish procedures to enable law enforcement officials to gain access to plaintext recovery systems upon presentation of a court order. The bill would direct the Attorney General to maintain data on the instances in which encryption impedes or obstructs the ability of DOJ to enforce criminal laws. Finally, the bill would establish criminal penalties and fines for the use of encryption technologies to further a crime, for the unlawful access of encrypted information, or for the unlawful sale of encryption technologies.

Estimated cost to the Federal Government

Spending Subject to Appropriation

Under current policy, BXA would likely spend about $900,000 a year, totaling $4.5 million over the 1998–2002 period, to monitor exports of encryption products. Assuming appropriation of the necessary amounts, CBO estimates that enacting H.R. 695 would increase BXA's encryption-related costs to about $6.6 million over the same period. That cost consists of two components: (1) costs to monitor encryption exports, and (2) costs for the new key management system. H.R. 695 would authorize the Department of Commerce through BXA to exempt encryption products with plaintext recovery systems from certain export licensing requirements after January 31, 2000. As a result, CBO estimates that the agency's cost to monitor encryption exports would decrease from about $900,000 in fiscal years 1998 and 1999 to about $650,000 in fiscal year 2000 and $500,000 in each year thereafter, for a five-year total of about $3.5 million. H.R. 695 also would require the agency to establish and maintain a key management system. Based on information from BXA, CBO estimates that establishing and maintaining this system would cost BXA about $500,000 in fiscal year 1998 and $600,000 in each year thereafter, for a five-year total of about $3.1 million.

H.R. 695 would require the Department of Justice to collect and maintain data on the instances in which encryption impedes or obstructs the ability of the agency to enforce criminal laws. The agency is uncertain as to how much it would cost to track such classified information nationwide. For the purposes of this estimate, CBO projects that collecting and maintaining the data would cost

DOJ between $500,000 and $1 million a year, assuming appropriation of the necessary amounts.

Direct Spending and Revenues

Enacting H.R. 695 would affect direct spending and receipts through the imposition of criminal fines for the use of encryption technologies to further a crime, for the unlawful access of encrypted information, and for the unlawful sale of encryption technologies. CBO estimates that collections from such fines are likely to be negligible, however, because the federal government would probably not pursue many cases under the bill. Any such collections would be deposited in the Crime Victims Fund and spent the following year. Because the increase in direct spending would be the same amount as the amount of fines collected with a one-year lag, the additional direct spending also would be negligible.

The costs of this legislation fall within budget functions 370 (commerce and housing credit) and 750 (administration of justice).

Pay-as-you-go considerations: Section 252 of the Balanced Budget and Emergency Deficit Control Act of 1985 sets up pay-as-you-go procedures for legislation affecting direct spending or receipts. H.R. 695 would affect direct spending and receipts through the imposition of criminal fines and the resulting spending from the Crime Victims Fund. CBO estimates, however, that any collections and spending resulting from such fines would not be significant.

Estimated impact on State, local, and tribal governments: H.R. 695 contains an intergovernmental mandate as defined in UMRA, because state and local governments that offer Internet access to their citizens would meet the bill's definition of "network service provider." As such, they would be required to ensure that any encryption products or services they provide enable the immediate decryption or access to the plaintext of encrypted data. At the present time, CBO is unsure of how many states and localities offer Internet access, as well as the steps these governments would take to comply with the mandate. CBO therefore cannot estimate the cost of complying with the mandate at this time and cannot determine whether the threshold established in UMRA would be exceeded.

Estimated impact on the private sector: H.R. 695 would establish controls on domestic encryption technology. Specifically, the bill would require sellers of encryption products to include features or functions that permit duly authorized individuals to gain immediate access to the encrypted material without the knowledge or cooperation of the user of those products. Thus, it would impose a federal private-sector mandate on network service providers and manufacturers, distributors, and importers of encryption products. CBO estimates that the total direct cost of complying with this mandate would exceed the statutory threshold ($100 million in 1996, adjusted annually for inflation) for private-sector mandates established in UMRA.

Section 4 of UMRA excludes from consideration any provisions that are considered necessary for national security purposes. Such provisions are found in Title III, Exports of Encryption.

CBO's full analysis of the costs of the intergovernmental and private-sector mandates will be provided under separate cover.

Previous CBO estimate: CBO provided cost estimates for H.R. 695 as ordered reported by the House Committee on the Judiciary on May 14, 1997, by the House Committee on International Relations on July 22, 1997, and by the House Committee on National Security on September 9, 1997. Assuming appropriation of the necessary amounts, CBO estimates that costs over the 1998–2002 period would total between $5 million and $7 million for the Judiciary Committee's version, about $2.2 million for the International Relations Committee's version, and about $4.5 million for the National Security Committee's version. In comparison, CBO estimates that enacting this version of the bill would cost between $9 million and $11.6 million and that spending under current policies would total $4.5 million.

Estimate prepared by: Federal Costs: Rachel Forward; Revenues: Alyssa Trzeszkowski; Impact on State, Local, and Tribal Governments; Pepper Santalucia; and Impact on the Private Sector: Jean Wooster.

Estimate approved by: Paul N. Van de Water, 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 defence 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 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 (new matter is printed in italic and existing law in which no change is proposed is shown in roman):

TITLE 18, UNITED STATES CODE

* * * * * * *

PART I—CRIMES

* * * * * * *

* * * * * * *

CHAPTER 122—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 alone shall not constitute 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. Unlawful sale of encryption

Whoever, after January 31, 2000, sells in interstate or foreign commerce any encryption product that does not include features or functions permitting duly authorized persons immediate access to plaintext or immediate decryption capabilities shall be imprisoned for not more than 5 years, fined under this title, or both.

§2804. Encryption products manufactured and intended for use in the United States

(a) PUBLIC NETWORK SERVICE PROVIDERS.—After January 31, 2000, public network service providers offering encryption products or encryption services shall ensure that such products or services enable the immediate decryption or access to plaintext of the data, including communications, encrypted by such products or services on the public network upon receipt of a court order or warrant, pursuant to section 2806.

(b) MANUFACTURERS, DISTRIBUTORS, AND IMPORTERS.—After January 31, 2000, it shall be unlawful for any person to manufacture for distribution, distribute, or import encryption products intended for sale or use in the United States, unless that product—

(1) includes features or functions that provide an immediate access to plaintext capability, through any means, mechanism, or technological method that—

(A) permits immediate decryption of the encrypted data, including communications, upon the receipt of decryption information by an authorized party in possession of a facially valid order issued by a court of competent jurisdiction; and

(B) allows the decryption of encrypted data, including communications, without the knowledge or cooperation of the person being investigated, subject to the requirements set forth in section 2806;

(2) can be used only on systems or networks that include features or functions that provide an immediate access to plaintext capability, through any means, mechanism, or technological method that—

(A) permits immediate decryption of the encrypted data, including communications, upon the receipt of decryption information by an authorized party in possession of a

facially valid order issued by a court of competent jurisdiction; and

(B) allows the decryption of encrypted data, including communications, without the knowledge or cooperation of the person being investigated, subject to the requirements set forth in section 2806; or

(3) otherwise meets the technical requirements and functional criteria promulgated by the Attorney General under subsection (c).

(c) ATTORNEY GENERAL CRITERIA.—

(1) PUBLICATION OF REQUIREMENTS.—Within 180 days after the date of the enactment of this chapter, the Attorney General shall publish in the Federal Register technical requirements and functional criteria for complying with the decryption requirements set forth in this section.

(2) PROCEDURES FOR ADVISORY OPINIONS.—Within 180 days after the date of the enactment of this chapter, the Attorney General shall promulgate procedures by which data network service providers and encryption product manufacturers, sellers, re-sellers, distributors, and importers may obtain advisory opinions as to whether an encryption product intended for sale or use in the United States after January 31, 2000, meets the requirements of this section and the technical requirements and functional criteria promulgated pursuant to paragraph (1).

(3) PARTICULAR METHODOLOGY NOT REQUIRED.—Nothing in this chapter or any other provision of law shall be construed as requiring the implementation of any particular decryption methodology in order to satisfy the requirements of subsections (a) and (b), or the technical requirements and functional criteria required by the Attorney General under paragraph (1).

(d) USE OF PRIOR PRODUCTS LAWFUL.—After January 31, 2000, it shall not be unlawful to use any encryption product purchased or in use prior to such date.

§2805. Injunctive relief and proceedings

(a) INJUNCTION.—Whenever it appears to the Secretary or the Attorney General that any person is engaged in, or is about to engage in, any act that constitutes, or would constitute, a violation of section 2804, the Attorney General may initiate a civil action in a district court of the United States to enjoin such violation. Upon the filing of the complaint seeking injunctive relief by the Attorney General, the court shall automatically issue a temporary restraining order against the party being sued.

(b) BURDEN OF PROOF.—In a suit brought by the Attorney General under subsection (a), the burden shall be upon the Government to establish by a preponderance of the evidence that the encryption product involved does not comport with the requirements set forth by the Attorney General pursuant to section 2804 providing for immediate access to plaintext by Federal, State, or local authorities.

(c) CLOSING OF PROCEEDINGS.—(1) Upon motion of the party against whom injunction is being sought—

(A) any or all of the proceedings under this section shall be closed to the public; and

(B) public disclosure of the proceedings shall be treated as contempt of court.

(2) Upon a written finding by the court that public disclosure of information relevant to the prosecution of the injunction or relevant to a determination of the factual or legal issues raised in the case would cause irreparable or financial harm to the party against whom the suit is brought, or would otherwise disclose proprietary information of any party to the case, all proceedings shall be closed to members of the public, except the parties to the suit, and all transcripts, motions, and orders shall be placed under seal to protect their disclosure to the general public.

(d) ADVISORY OPINION AS DEFENSE.—It is an absolute defense to a suit under this subsection that the party against whom suit is brought obtained an advisory opinion from the Attorney General pursuant to section 2804(c) and that the product at issue in the suit comports in every aspect with the requirements announced in such advisory opinion.

(e) BASIS FOR PERMANENT INJUNCTION.—The court shall issue a permanent injunction against the distribution of, and any future manufacture of, the encryption product at issue in the suit filed under subsection (a) if the court finds by a preponderance of the evidence that the product does not meet the requirements set forth by the Attorney General pursuant to section 2804 providing for immediate access to plaintext by Federal, State, or local authorities.

(f) APPEALS.—Either party may appeal, to the appellate court with jurisdiction of the case, any adverse ruling by the district court entered pursuant to this section. For the purposes of appeal, the parties shall be governed by the Federal Rules of Appellate Procedure, except that the Government shall file its notice of appeal not later than 30 days after the entry of the final order on the docket of the district court. The appeal of such matter shall be considered on an expedited basis and resolved as soon as practicable.

§2806. Court order access to plaintext

(a) COURT ORDER.—(1) A court of competent jurisdiction shall issue an order, ex parte, granting an investigative or law enforcement officer immediate 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 or foreign counterintelligence 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 or foreign counterintelligence 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 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) OTHER ORDERS.—An attorney for the Government may make application to a district court of the United States for an order under subsection (a), upon a request from a foreign country pursuant to a Mutual Legal Assistance Treaty with such country that is in effect at the time of the request from such country.

(c) 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 shall 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.

(d) 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.

(e) 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 that would otherwise remain encrypted.

§2807. 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 2806 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 that 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, have 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. On an ex parte showing of good cause to a court of competent jurisdiction, the serving of the inventory required by this subsection may be postponed.

(b) ADMISSION INTO EVIDENCE.—The contents 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 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.

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

(d) 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 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 unlawfully decrypted or accessed;

(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.

(e) 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 (d), or the denial of an application for an order under section 2806, if the

United States attorney 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.

(f) CIVIL ACTION FOR VIOLATION.—Except as otherwise provided in this chapter, any person described in subsection (g) 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.

(g) COVERED PERSONS.—Subsection (f) 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.

(h) LIMITATION.—A civil action under subsection (f) 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.

(i) 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.

(j) 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 a timely or reasonable fashion. The court, upon notice to the Government, shall decide such motion expeditiously.

(k) 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.

§2808. 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 use such plaintext or decryption information for the purposes of conducting a lawful criminal investigation or foreign counterintelligence 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 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) 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 2806, a key recovery agent may not disclose decryption information stored with the key recovery agent by a person unless the disclosure is—

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

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

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

(A) the person who supplied the information is given reasonable notice, by the person seeking the disclosure, of the

court proceeding relevant to the issuance of the court order; and

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

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

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

§2809. Identification of decryption information

(a) IDENTIFICATION.—To avoid inadvertent disclosure, 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 provided 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 facilities and in a method so as to reasonably assure that inadvertent disclosure does not occur.

§2810. Unlawful export of certain encryption products

Whoever, after January 31, 2000, knowingly exports an encryption product that does not include features or functions providing duly authorized persons immediate access to plaintext or immediate decryption capabilities, as required under law, shall be imprisoned for not more than 5 years, fined under this title, or both.

§2811. Definitions

The definitions set forth in section 101 of the Security and Freedom through Encryption ("SAFE") Act of 1997 shall apply to this chapter.

* * * * * * *

ADDITIONAL VIEWS OF REPRESENTATIVES DICKS, SKELTON, AND BISHOP

In considering H.R. 695, we used six principles as a guide through the difficult and complex issues posed by encryption technology.

First, Congress should take no action to impair or abridge the rights, liberties, and privacy of the American people guaranteed by our constitution.

Second, Congress has an obligation to ensure that the ability of law enforcement agencies to provide protection against violent criminals, terrorists, narcotics dealers, organized crime syndicates, and espionage is not unwisely diminished.

Third, there is an equally compelling need to guarantee the protection of electronic information for the security of the nation, for the privacy and protection of our citizens and their property, and for the prosperity of the country through a new form of commerce.

Fourth, Congress must protect our ability to collect intelligence to support national defense, diplomacy, and law enforcement.

Fifth, we must not disadvantage, and should as best we can promote, American workers and companies seeking to maintain dominance in information technologies.

Finally, our domestic and foreign policy in this area should, to the maximum extent possible, be consistent and reinforcing.

It is commonly asserted that these principles are substantially at odds with one another, such that any consistent policy position must entail compromises among them—perhaps fatal ones. We do not believe that is true and am convinced that the substitute the Committee adopted is faithful to all these principles.

In contrast, H.R. 695 as referred to the Committee is in conflict with several of the foregoing principles. H.R. 695 is incompatible with national security because it essentially does away with the export control process. Gutting the export control process would also have serious foreign policy consequences, undermining administration attempts to develop an international consensus on encryption policy and perhaps prompting other countries to erect import barriers to U.S. encryption products and associated hardware and software systems. The bill would do nothing to foster a domestic key management infrastructure, which the administration, the Committee, and much of industry believe is important for the rapid expansion of electronic commerce. The bill is deficient also in that it would not help law enforcement overcome the negative consequences of the inevitable proliferation of strong encryption.

Without legislative intervention, in the near future the nation's police departments and the FBI will not need to bother to install wiretaps because everything they hear will be encrypted. Proponents of H.R. 695 as referred to the Committee acknowledge this problem but argue that the law enforcement interest is a narrow

one and should be sacrificed. Others assert that it is futile to try to protect law enforcement equities either because unbreakable encryption will proliferate no matter what the government does, or that any government regulatory actions will do much more harm than good. With regard to export controls, proponents of H.R. 695 contend that without an inclusive international compact to regulate encryption, it is pointless, crippling to U.S. industry, to maintain a rigid export control regime. They assert that there is no reason to believe that any international consensus is likely, and that U.S. industry already faces an imminent competitive threat.

We reject these arguments. Communications intercepts are a critically important and effective law enforcement tool. While it is true that the government cannot hope to prevent determined and resourceful criminals, terrorists, and others from using unbreakable encryption to hide their activities, these elements must interact with society at large, and therefore must conduct most of their business using standard forms of electronic commerce and communication. If the latter provide lawful access to the plaintext of encrypted information, or to decryption information pursuant to court order, law enforcement will be able to conduct investigations effectively. Thus it is neither necessary nor expected that the Committee substitute would eradicate unapproved encryption capabilities.

In terms of the practicality of regulating encryption products, we recognize also that it is not a certainty that the burden the substitute would place on the marketplace to provide some form of access for communications will prove to be marginally costly or inconvenient. We acknowledge the possibility that critics could be right—that these requirements will be unwieldy or expensive, or both. But it is far from clear today that the critics are right, and the administration predicts modest annual user costs. If the law is to err, however, we strongly favor doing it on the side of ensuring that our public safety and national security officials can continue to do their jobs effectively.

We recognize that there is no certainty of success in the attempt to convince the other advanced nations of the need to control encryption to protect law enforcement as we propose to do. The United States cannot hope to convince others to take this path, however, if it decides first to flood the world with unbreakable encryption, and second to proclaim that domestic controls are somewhat incompatible with liberty.

Furthermore, any fair assessment of the status of discussions with other advanced nations on this issue would conclude that success is quite feasible. Similarly, claims about the availability of truly strong encryption products on the world market that users can readily access and employ are clearly exaggerated. Finally, as the section-by-section analysis in this report explains, the Committee substitute provides for the export of encryption products with an access "on-off switch," in effect allowing industry to export unbreakable encryption to countries that have no requirement for law enforcement access to plaintext.

Critics also assert that it is unreasonable for Congress to consider levying a mandate on the private sector in information technology to provide a means for lawful access to encrypted informa-

tion. In fact, there is an important precedent for such action. Just a few years ago, law enforcement agencies were similarly faced with the prospect of loosing the ability to intercept communications because of the astonishing complexity of the nation's emerging digital telecommunications networks—even when the underlying information is unencrypted. Congress met the political challenge of supporting law enforcement in this instance by requiring communications service providers to install capabilities to permit effective wiretaps. This digital telephony act also required telephone communications service providers to provide access to plaintext to duly authorized law enforcement agencies where the service providers offered their customers encryption capabilities that could be decrypted. The point is that Congress was willing to do what was right when the issue was clear.

We face another such challenge today. We believe that my colleagues will respond appropriately once they realize what is at stake. The place to start that educational process is here, with the Committee substitute. We do not think that a fair analysis of the substitute could conclude that it would compromise the rights of our citizens by insisting that law enforcement agencies merely retain their current ability to gather evidence through judicially sanctioned electronic surveillance.

NORM DICKS.
IKE SKELTON.
SANFORD D. BISHOP, Jr.

ADDITIONAL VIEWS OF REPRESENTATIVES HARMAN, SKAGGS, AND DIXON

The issue of encryption is one of the most difficult we have faced in our careers in the Congress. The technical complexities of algorithms and bit strength are the least of the problem. What is most challenging is discovering a way to balance competing policy concerns in the face of a rapidly evolving electronic infrastructure.

We are convinced that H.R. 695 as introduced and reported from the Committees on Judiciary and International Relations is neither the right answer, nor a comprehensive approach to the challenges we face. As members of the Permanent Select Committee on Intelligence we believe U.S. policy should balance sometimes conflicting goals: protecting public computer networks from the threats of terrorists and other criminals through the use of strong encryption; promoting the economic competitiveness and the research and development breakthroughs of our vital information technology industry; encouraging the legal framework necessary for robust and reliable electronic commerce; and helping preserve public safety and national security.

H.R. 695 as introduced was intended to promote economic competitiveness but it does little to address the strongly expressed concerns of law enforcement officials from around the country that the legislation would eliminate the possibility of electronic surveillance under lawful court order.

The substitute the Committee has ordered reported is an attempt to address all of the issues in the debate comprehensively. Yet, it has been developed under an extremely short time frame, subject to a limited referral. We believe the legislation is too sweeping, particularly in placing new requirements on the manufacture, sale, and import of encryption products in the United States.

While we want United States law enforcement and national security agencies, working under proper oversight, to have the tools they need to respond to threats to the public safety and national security, the requirement in the legislation that encryption products manufactured and distributed for sale or use, or imported for sale or use after January 31, 2000, include features or functions that provide, upon presentment of a court order, immediate access to plaintext data or decryption information from the encryption provider, raises a host of new questions and issues that need further exploration. We are worried less about the narrow question of technical feasibility than how such a requirement would implicate valid concerns about privacy, abuse of official authority, and the inherent security of data security services. We are concerned whether the legislation's provision on imports might be interpreted to mean an individual on the Internet downloading encryption from a foreign country was violating the law and about where the line would

be drawn on the prohibited distribution of encryption products not meeting the bill's legal requirements.

The substitute is intended to put in place a legal framework for, and safeguards on, law enforcement access to encrypted electronic information. This is positive. Imposing new criminal penalties for the invasion of privacy relating to the misuse of decryption information is appropriate to ensure that government officials who gain access to information on the electronic network do not exceed their lawful authority. Likewise, we support requiring a verifiable audit trail whenever government officials obtain access to plaintext and decrypted information, regardless of whether or not a recovery-capable mandate on encryption is enacted. We are fast approaching what Kenneth Flamm of the Brookings Institution calls "a digital future in which almost everything * * * is stored or communicated electronically, connected to or accessible through some computer network." It is time to take action on these issues.

In addition, we recognize that the issues raised in this debate are international in scope. Given the availability of encryption technology abroad, and the ease of its dissemination, a unilateral export control policy on encryption will not work. Therefore, we must encourage, if not direct, the Administration to monitor closely international developments and to engage other countries in working out a multilateral approach to this issue.

Recent events suggest passage of H.R. 695 as originally conceived is highly unlikely in the House of Representatives. We believe there now needs to be a very careful and deliberative effort to fashion balanced legislation. The information technology industry should suggest targeted legislative and regulatory amendments which will meet its need for fewer uncertainties in the export control process, while still allowing for regulatory flexibility as technology advances. Privacy advocates should recognize that government access to information residing on the electronic infrastructure in order to protect public safety is legitimate within reasonable constraints, and should propose what those reasonable constraints should be. Law enforcement officials should carefully evaluate where their highest priorities lie in protecting the public safety and preventing crime. The Administration should redouble its efforts to secure international agreements of mutual recognition of encryption management infrastructures to safeguard the privacy of United States citizens and enhance U.S. information security needs in electronic commerce. Continued stalemate on balancing the competing policy concerns is not in the interests of industry, law enforcement or the American people.

JANE HARMAN.
DAVID E. SKAGGS.
JULIAN C. DIXON.

ADDITIONAL VIEWS OF REPRESENTATIVE NANCY PELOSI

I oppose the substitute to H.R. 695 ordered reported from the Permanent Select Committee on Intelligence. While there are indeed serious national security and law enforcement issues at stake in this debate, there are also serious questions about the impact of this legislation on the civil liberties on which this nation is based. A balance must be struck. The bill passed by the Committee does not strike the requisite balance.

I was very concerned about the lack of an audit mechanism in the Committee's substitute as proposed and am pleased that the bill was amended to require an electronic audit trail, to ensure that there is accountability when an investigative or law enforcement officer obtains access to the plaintext of otherwise encrypted information or the provision of decryption information.

Among the reasons I oppose the bill are the following:

With respect to domestic controls, the ramifications of enacting a requirement that encryption products manufactured, distributed or imported in the United States after January 2000 contain features that provide, upon presentment of a court order, immediate plaintext access or decryption information, are not well understood. It is not clear such a requirement could pass constitutional muster, particularly where it might place restrictions on the distribution of encryption algorithms or the free flow of ideas among scientists working in the area of information technology. Indeed imposing domestic controls runs counter to the first recommendation of the National Research Council's widely-respected CRISIS report ("Cryptography's Role in Security in the Information Society," June 1996) that no law bar the manufacture, sale or use of any form of encryption in the United States. Despite the many provisions of the legislation designed to place civil and criminal penalties on official misuse of decryption information, and provide privacy protections to those who encrypt information, further debate is needed on whether the legal framework governing lawful wiretaps is the appropriate model for the 21st Century as so much information concerning our personal and economic lives is connected and accessible on-line.

With respect to export controls, the legislation would force U.S. manufacturers to include features that could provide plaintext access or decryption information in encryption products exported overseas. Although the legislation allows these features to be enabled at the foreign purchaser's option, and does not require any keys or recovery information be held in escrow in the United States, demanding recovery capable features in exportable U.S. technology may provide repressive totalitarian regimes a new method of control over dissidents and human rights advocates who today evade surveillance by utilizing unbreakable encryption on the Internet.

Also of concern is the impact of certain of the substitute's provisions on human rights activists in authoritarian countries. Human rights activists worldwide are using cryptography to protect their sources from reprisals by governments that violate human rights. Under the Committee substitute, the U.S. government can get a court order for violating the security of communications "upon a request from a foreign country pursuant to a Mutual Legal Assistance Treaty." This provision will permit governments to breach the protection of confidential sources, thereby both endangering human rights activists using electronic communications and discouraging people who know of human rights violations to speak about them, even in private. Authoritarian governments often define the activities of those who dare to speak out against them as "treason" or "revealing classified information," crimes recognized by the U.S. government. Under the Committee substitute, legitimate human rights activists, who now communicate safely through the Internet with strong encryption protection, will no longer have that safety.

In addition, the legislation enshrines the broad concept that all decisions of the Secretary of Commerce with respect to the export of encryption products are not subject to judicial review. If the question at hand has to do with national security implications, the President could waive judicial review on a case-by-case basis as needed, rather than Congress acting to grant a blanket waiver of a citizen's right to recourse to the legal system.

The serious issues involving national security and public safety could have been resolved with a more narrowly targeted approach. I hope efforts will be made to craft a consensus measure before H.R. 695 is considered on the floor of the House of Representatives.

NANCY PELOSI.

LETTERS FROM LAW ENFORCEMENT OFFICERS AND THE SECRETARY OF DEFENSE

THE SECRETARY OF DEFENSE,
Washington, DC, July 21, 1997.

DEAR MEMBER OF CONGRESS: Recently you received a letter from the nation's senior law enforcement officials regarding U.S. encryption policies. I am writing today to express my strong support for their views on their important issue.

As you know, the Department of Defense is involved on a daily basis in countering international terrorism, narcotics trafficking, and the proliferation of weapons of mass destruction. The spread of unbreakable encryption, as a standard feature of mass market communication products, presents a significant threat to the ability of the U.S. and its allies to monitor the dangerous groups and individuals involved in these activities. Passage of legislation which effectively decontrols commercial encryption exports would undermine U.S. efforts to foster the use of strong key recovery encryption domestically and abroad. Key recovery products will preserve governments' abilities to counter worldwide terrorism, narcotics trafficking and proliferation.

It is also important to note that the Department of Defense relies on the Federal Bureau of Investigation for the apprehension and prosecution of spies. Sadly, there have been over 60 espionage convictions of federal employees over the last decade. While these individuals represent a tiny minority of government employees, the impact of espionage activities on our nation's security can be enormous. As the recent arrests of Nicholson, Pitts and Kim clearly indicate, espionage remains a very serious problem. Any policies that detract from the FBI's ability to perform its vital counterintelligence function, including the ability to perform wiretaps, inevitably detract from the security of the Department of Defense and the nation.

Encryption legislation must also address the nation's domestic information security needs. Today, approximately 95% of DoD communications rely on public networks; other parts of government, and industry, are even more dependent on the trustworthiness of such networks. Clearly, we must ensure that encryption legislation addresses these needs. An approach such as the one contained in S. 909 can go a long way toward balancing the need for strong encryption with the need to preserve national security and public safety. I hope that you will work with the Administration to enact legislation that addresses these national security concerns as well as the rights of the American people.

I appreciate your consideration of these views.

Sincerely,

BILL COHEN.

OFFICE OF THE ATTORNEY GENERAL,
Washington, DC, July 18, 1997.

DEAR MEMBER OF CONGRESS: Congress is considering a variety of legislative proposals concerning encryption. Some of these proposals would, in effect, make it impossible for the Federal Bureau of Investigation (FBI), Drug Enforcement Administration (DEA), Secret Service, Customs Service, Bureau of Alcohol, Tobacco and Firearms, and other federal, state, and local law enforcement agencies to lawfully gain access to criminal telephone conversations or electronically stored evidence possessed by terrorists, child pornographers, drug kingpins, spies and other criminals. Since the impact of these proposals would seriously jeopardize public safety and national security, we collectively urge you to support a different, balanced approach that strongly supports commercial and privacy interests but maintains our ability to investigate and prosecute serious crimes.

We fully recognize that encryption is critical to communications security and privacy, and that substantial commercial interests are at stake. Perhaps in recognition of these facts, all the bills being considered allow market forces to shape the development of encryption products. We, too, place substantial reliance on market forces to promote electronic security and privacy, but believe that we cannot rely solely on market forces to protect the public safety and national security. Obviously, the government cannot abdicate its solemn responsibility to protect public safety and national security.

Currently, of course, encryption is not widely used, and most data is stored, and transmitted, in the clear. As we move from a plaintext world to an encrypted one, we have a critical choice to make: we can either (1) choose robust, unbreakable encryption that protects commerce and privacy but gives criminals a powerful new weapon, or (2) choose robust, unbreakable encryption that protects commerce and privacy and gives law enforcement the ability to protect public safety. The choice should be obvious and it would be a mistake of historic proportions to do nothing about the dangers to public safety posed by encryption without adequate safeguards for law enforcement.

Let there be no doubt: without encryption safeguards, all Americans will be endangered. No one disputes this fact; not industry, not encryption users, no one. We need to take definitive actions to protect the safety of the public and security of the nation. That is why law enforcement at all levels of government—including the Justice Department, Treasury Department, the National Association of Attorneys General, International Association of Chiefs of Police, the Major City Chiefs, the National Sheriffs' Association, and the National District Attorneys Association—are so concerned about this issue.

We all agree that without adequate legislation, law enforcement in the United States will be severely limited in its ability to combat the worst criminals and terrorists. Further, law enforcement agrees that the widespread use of robust non-key recovery encryption ultimately will devastate our ability to fight crime and prevent terrorism.

Simply stated, technology is rapidly developing to the point where powerful encryption will become commonplace both for routine telephone communications and for stored computer data. Without legislation that accommodates public safety and national security concerns, society's most dangerous criminals will be able to communicate safely and electronically store data without fear of discovery. Court orders to conduct electronic surveillance and court-authorized search warrants will be ineffectual, and the Fourth Amendment's carefully-struck balance between ensuring privacy and protecting public safety will be forever altered by technology. Technology should not dictate public policy, and it should promote, rather than defeat, public safety.

We are not suggesting the balance of the Fourth Amendment be tipped toward law enforcement either. To the contrary, we only seek the status quo, not the lessening of any legal standard or the expansion of any law enforcement authority. The Fourth Amendment protects the privacy and liberties of our citizens but permits law enforcement to use tightly controlled investigative techniques to obtain evidence of crimes. The result has been the freest country in the world with the strongest economy.

Law enforcement has already confronted encryption in high-profile espionage, terrorist, and criminal cases. For example:

An international terrorist was plotting to blow up 11 U.S.-owned commercial airliners in the Far East. His laptop computer, which was seized in Manila, contained encrypted files concerning this terrorist plot;

A subject in a child pornography case used encryption in transmitting obscene and pornographic images of children over the Internet; and

A major international drug trafficking subject recently used a telephone encryption device to frustrate court-approved electronic surveillance.

And this is just the tip of the iceberg. Convicted spy Aldrich Ames, for example, was told by the Russian Intelligence Service to encrypt computer file information that was to be passed to them.

Further, today's international drug trafficking organizations are the most powerful, ruthless and affluent criminal enterprises we have ever faced. We know from numerous past investigations that they have utilized their virtually unlimited wealth to purchase sophisticated electronic equipment to facilitate their illegal activities. This has included state of the art communication and encryption devices. They have used this equipment as part of their command and control process for their international criminal operations. We believe you share our concern that criminals will increasingly take advantage of developing technology to further insulate their violent and destructive activities.

Requests for cryptographic support pertaining to electronic surveillance interceptions from FBI Field Offices and other law enforcement agencies have steadily risen over the past several years. There has been an increase in the number of instances where the FBI's and DEA's court-authorized electronic efforts were frustrated by the use of encryption that did not allow for law enforcement access.

There have also been numerous other cases where law enforcement, through the use of electronic surveillance, has not only solved and successfully prosecuted serious crimes but has also been able to prevent life-threatening criminal acts. For example, terrorists in New York were plotting to bomb the United Nations building, the Lincoln and Holland Tunnels, and 26 Federal Plaza as well as conduct assassinations of political figures. Court-authorized electronic surveillance enabled the FBI to disrupt the plot as explosives were being mixed. Ultimately, the evidence obtained was used to convict the conspirators. In another example, electronic surveillance was used to stop and then convict two men who intended to kidnap, molest, and kill a child. In all of these cases, the use of encryption might have seriously jeopardized public safety and resulted in the loss of life.

To preserve law enforcement's abilities, and to preserve the balance so carefully established by the Constitution, we believe any encryption legislation must accomplish three goals in addition to promoting the widespread use of strong encryption. It must establish:

A viable key management infrastructure that promotes electronic commerce and enjoys the confidence of encryption users;

A key management infrastructure that supports a key recovery scheme that will allow encryption users access to their own data should the need arise, and that will permit law enforcement to obtain lawful access to the plaintext of encrypted communications and data; and

An enforcement mechanism that criminalizes both improper use of encryption key recovery information and the use of encryption for criminal purposes.

Only one bill, S. 909 (the McCain/Kerrey/Hollings bill), comes close to meeting these core public safety, law enforcement, and national security needs. The other bills being considered by Congress, as currently written, risk great harm to our ability to enforce the laws and protect our citizens. We look forward to working to improve the McCain/Kerrey/Hollings bill.

In sum, while encryption is certainly a commercial interest of great importance to this Nation, it is not solely a commercial or business issue. Those of us charged with the protection of public safety and national security, believe that the misuse of encryption

technology will become a matter of life and death in many instances. That is why we urge you to adopt a balanced approach that accomplishes the goals mentioned above. Only this approach will allow police departments, attorneys general, district attorneys, sheriffs, and federal authorities to continue to use their most effective investigative techniques, with court approval, to fight crime and espionage and prevent terrorism.

Sincerely yours,

JANET RENO,
Attorney General.
LOUIS FREEH,
Director, Federal Bureau of Investigation.
THOMAS A. CONSTANTINE,
Director, Drug Enforcement Administration.
RAYMOND W. KELLY,
Undersecretary for Enforcement, U.S. Department of the Treasury.
JOHN W. MAGAW,
Director, Bureau of Alcohol, Tobacco and Firearms.
BARRY MCCAFFREY,
Director, Office of National Drug Control Policy.
LEWIS C. MERLETTI,
Director, United States Secret Service.
GEORGE J. WEISE,
Commissioner, United States Customs Service.

INTERNATIONAL ASSOCIATION OF
CHIEFS OF POLICE,
Alexandria, VA, July 21, 1997.

DEAR MEMBER OF CONGRESS: Enclosed is a letter sent to you by the Attorney General, the Director of National Drug Control Policy and all the federal law enforcement heads concerning encryption legislation being considered by congress. Collectively we, the undersigned, represent over 17,000 police departments including every major city police department, over 3,000 sheriffs departments, nearly every district attorney in the United States and all of the state Attorneys General. We fully endorse the position taken by our federal counterparts in the enclosed letter. As we have stated many times, Congress must adopt a balanced approach to encryption that fully addresses public safety concerns or the ability of state and local law enforcement to fight crime and drugs will be severely damaged.

Any encryption legislation that does not ensure that law enforcement can gain timely access to the plaintext of encrypted conversations and information by established legal procedures will cause grave harm to public safety. The risk cannot be left to the uncer-

tainty of market forces or commercial interests as the current legislative proposals would require. Without adequate safeguards, the unbridled use of powerful encryption soon will deprive law enforcement of two of its most effective tools, court authorized electronic surveillance and the search and seizure of information stored in computers. This will substantially tip the balance in the fight against crime towards society's most dangerous criminals as the information age develops.

We are in unanimous agreement that congress must adopt encryption legislation that requires the development, manufacture, distribution and sale of only key recovery products and we are opposed to the bills that do not do so. Only the key recovery approach will ensure that law enforcement can continue to gain timely access to the plaintext of encrypted conversations and other evidence of crimes when authorized by a court to do so. If we lose this ability—and the bills you are considering will have this result—it will be a substantial setback for law enforcement at the direct expense of public safety.

Sincerely yours,

DARRELL L. SANDERS,
President, International Association of Chiefs of Police.
JAMES E. DOYLE,
President, National Association of Attorneys General.
FRED SCORALIE,
President, National Sheriffs' Association.
WILLIAM L. MURPHY,
President, National District Attorneys Association.

MAJOR CITIES CHIEFS,
Chicago IL, July 24, 1997.

Hon. ORRIN G. HATCH,
Chairman, Judiciary Committee, Senate Hart Office Building, Washington, DC.

DEAR MR. CHAIRMAN: The Major Cities Chiefs is a professional association of police executives representing the largest jurisdictions in the United States. The association provides a forum for urban police chiefs, sheriffs and other law enforcement chief executives to discuss common problems associated with protecting cites with populations exceeding 500,000 people.

Congress is considering a variety of legislative proposals concerning encryption. Some of these proposals would, in effect, make it impossible for law enforcement agencies across the country, both on the federal, state and local level, to lawfully gain access to criminal telephone conversations or electronically stored evidence. Since the impact of these proposals would seriously jeopardize public safety, our association urges you to support a balanced approach that strongly supports commercial and private interests but also main-

tains law enforcements ability to investigate and prosecute serious crime.

While we recognize that encryption is critical to communications security and privacy and that commercial interests are at stake, we all agree that without adequate legislation, law enforcement across the country will be severely limited in its ability to combat serious crime. The widespread use of non-key recovery encryption ultimately will eliminate our ability to obtain valuable evidence of criminal activity. The legitimate and lawful interception of communications, pursuant to a court order, for the most serious criminal acts will be meaningless because of our inability to decipher the evidence.

Encryption is certainly of great importance to the commercial interests across this country. However, public safety concerns are just as critical and we must not loose sight of this. The need to preserve an invaluable investigative tool is of the utmost importance in law enforcements ability to protect the public against serious crime.

Sincerely yours,

MATT L. RODRIGUEZ, *Chairman.*

NATIONAL DISTRICT
ATTORNEYS ASSOCIATION,
Alexandria, VA.

RESOLUTION

ENCRYPTION

Whereas, the introduction of digitally-based telecommunications technologies as well as the widespread use of computers and computer networks having encryption capabilities are facilitating the development and production of strong, affordable encryption products and services for private sector use; and

Whereas, on one hand the use of strong encryption products and services are extremely beneficial when used legitimately to protect commercially sensitive information and communications. On the other hand, the potential use of strong encryption products and services that do not allow for timely law enforcement decryption by a vast array of criminals and terrorist to conceal their criminal communications and information from law enforcement poses an extremely serious threat to public safety: and

Whereas, the law enforcement community is extremely concerned about the serious threat posed by the use of these strong encryption products and services that do not allow for authorization (court-authorized wiretaps or court-authorized search and seizure); and

Whereas, law enforcement fully supports a balanced encryption policy that satisfies both the commercial needs of industry for strong encryption while at the same time satisfying law enforcement's public safety needs for the timely decryption of encrypted criminal communications and information; and

Whereas, law enforcement has found that strong key recovery encryption products and services are clearly the best way, and per-

haps the only way, to achieve both the goals of industry and law enforcement; and

Whereas, government representatives have been working with industry to encourage the voluntary development, sale, and use of key recovery encryption products and services in its pursuit of a balanced encryption policy;

Be it resolved, That the National District Attorneys Association supports and encourages the development and adoption of a balanced encryption policy that encourages the development, sale, and use of key recovery encryption products and services, both domestically and abroad. We believe that this approach represents a policy that appropriately addresses both the commercial needs of industry while at the same time satisfying law enforcement's public safety needs.

ENCRYPTION

Whereas, the introduction of digitally-based telecommunications technologies, as well as the widespread use of computers and computer networks having encryption capabilities are facilitating the development and production of affordable and robust encryption products for private sector use; and

Whereas, on one hand encryption is extremely beneficial when used legitimately to protect commercially sensitive information and communications. On the other hand, the potential use of such encryption products by a vast array of criminals and terrorists to conceal their criminal communications and information from law enforcement poses an extremely serious threat to public safety; and

Whereas, the law enforcement community is extremely concerned about the serious threat posed by the use of robust encryption products that do not allow for law enforcement access and its timely decryption, pursuant to lawful authorization (court-authorized wiretaps or court-authorized search and seizure); and

Whereas, law enforcement fully supports a balanced encryption policy that satisfies both the commercial needs of industry for robust encryption while at the same time satisfying law enforcement's public safety needs; and

Whereas, law enforcement has found that robust key-escrow encryption is clearly the best way, and perhaps the only way, to achieve both the goals of industry and law enforcement; and

Whereas, government representatives have been working with industry to encourage the voluntary development, sale, and use of key-escrow encryption in its pursuit of a balanced encryption policy: Now, therefore, be it

Resolved, that the International Association of Chiefs of Police, duly assembled at its 103rd annual conference in Phoenix, Arizona supports and encourages the development and adoption of a key-escrow encryption policy, which we believe represents a policy that appropriately addresses both the commercial needs of industry while at the same time satisfying law enforcement's public safety needs and that we oppose any efforts, legislatively or otherwise, that would undercut the adoption of such a balanced encryption policy.

NATIONAL SHERIFFS' ASSOCIATION
CHIEFS OF POLICE,

RESOLUTION

DIGITAL TELECOMMUNICATIONS ENCRYPTION

Whereas, the introduction of digitally-based telecommunications technologies as well as the widespread use of computers and computer networks having encryption capabilities are facilitating the development and production of affordable and robust encryption products for private sector use: and

Whereas, on one hand, encryption is extremely beneficial when used legitimately to protect commercially sensitive information and communications. On the other hand, the potential use of such encryption products by a vast array of criminals and terrorists to conceal their criminal communications and information from law enforcement poses an extremely serious threat to public safety; and

Whereas, the law enforcement community is extremely concerned about the serious threat posed by the use of robust encryption products that do not allow for court authorized law enforcement access and its timely decryption, pursuant to lawful authorization; and

Whereas, law enforcement fully supports a balanced encryption policy that satisfies both the commercial needs of industry for robust encryption while at the same time satisfying law enforcement's public safety needs; and

Whereas, law enforcement has found that robust key-escrow encryption is clearly the best way, and perhaps the only way, to achieve both the goals of industry and law enforcement; and

Whereas, government representatives have been working with industry to encourage the voluntary development, sale and use of key-escrow encryption in its pursuit of a balanced encryption policy; and therefore, be it

Resolved That the National Sheriffs' Association supports and encourages the development and adoption of a key-escrow encryption policy which we believe represents a policy that appropriately addresses both the commercial needs of industry while at the same time satisfying law enforcement's public safety needs and that we oppose any efforts, legislatively or otherwise, that would undercut the adoption of such a balanced encryption policy.

IMPERIAL COUNTY SHERIFF,
CORONER'S OFFICE,
El Centro, CA, August 26, 1997.

Re Key recovery of encrypted data.

Hon. PORTER J. GOSS,
Chairman, Permanent Select Committee on Intelligence, Washington, DC.

DEAR CHAIRMAN GOSS: I join my associates in Federal law enforcement, as well as the International Association of Chiefs of Po-

lice, the National Sheriff's Association, and the National District Attorney's Association, in urging you to make provisions for key recovery of encrypted data. Both of you and your Committee are familiar with the technology and the issues, and I won't waste your time or attention in a lengthy discourse on what encryption or key recovery is. You know as much about the technology as I do.

Of particular interest to me is the ability of international drug cartels to thwart legitimate, court-sanctioned interception of criminal communications here along the border. Drug trafficking organizations are sophisticated, aggressive, and well-funded. They certainly are taking advantage today of encryption technology in our own country. Without provisions for key recovery, it will be virtually impossible for law enforcement to conduct criminal investigations of telecommunications activity or electronic data files. A simple solution is to require a provision in trade agreements which requires a trustworthy key agent to maintain the key to encrypted data. Such a requirement would still allow legitimate safeguarding of data, but would also allow law enforcement to crack coded information in criminal investigations and national security matters.

I would be pleased to discuss this vital matter with you and I will be appreciative of any consideration you may give this issue.

Sincerely,

OREN R. FOX, *Sheriff-Coroner.*

○

Document No. 8