106TH CONGRESS
1ST SESSION

H. R. 2616

To clarify the policy of the United States with respect to the use and export of encryption products, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

JULY 27, 1999

Mr. GOSS (for himself, Mr. DIXON, Mr. LEWIS of California, Mr. CASTLE, Mr. BOEHLERT, Mr. BASS, Mr. GIBBONS, Mr. LAHOOD, Mrs. WILSON, Mr. BISHOP, Mr. SISISKY, Mr. CONDIT, Mr. HASTINGS of Florida, Mr. GILMAN, Mr. OXLEY, and Mr. STEARNS) introduced the following bill; which was referred to the Committee on the Judiciary, and in addition to the Committees on International Relations, and Government Reform, for a period to be subsequently determined by the Speaker, in each case for consideration of such provisions as fall within the jurisdiction of the committee concerned

---

A BILL

To clarify the policy of the United States with respect to the use and export of encryption products, and for other purposes.

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

SECTION 1. SHORT TITLE; TABLE OF CONTENTS.

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

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

Sec. 1. Short title; table of contents.
Sec. 2. Statement of policy.
Sec. 3. Congressional findings.

TITLE I—DOMESTIC USES OF ENCRYPTION

Sec. 101. Definitions.
Sec. 102. Lawful use of encryption.
Sec. 103. Unlawful use of encryption.

TITLE II—GOVERNMENT PROCUREMENT

Sec. 201. Federal purchases of encryption products.
Sec. 202. Networks established with Federal funds.
Sec. 203. Government contract authority.
Sec. 204. Product labels.
Sec. 205. No private mandate.
Sec. 206. Exclusion.

TITLE III—EXPORTS OF ENCRYPTION

Sec. 301. Exports of encryption.
Sec. 302. License exception for certain encryption products.
Sec. 303. Discretionary authority.
Sec. 304. Expedited review authority.
Sec. 305. Encryption licenses required.
Sec. 306. Encryption Industry and Information Security Board.

TITLE IV—LIABILITY LIMITATIONS

Sec. 401. Compliance with court order.
Sec. 402. Compliance defense.
Sec. 403. Good faith defense.

TITLE V—INTERNATIONAL AGREEMENTS

Sec. 501. Sense of Congress.
Sec. 502. Failure to negotiate.
Sec. 503. Report to Congress.

TITLE VI—MISCELLANEOUS PROVISIONS

Sec. 601. Effect on law enforcement activities.
Sec. 602. Interpretation.
Sec. 603. FBI technical support.
Sec. 604. Severability.

SEC. 2. STATEMENT OF POLICY.

It is the policy of the United States to protect public computer networks through the use of strong encryption

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

SEC. 3. CONGRESSIONAL FINDINGS.

The Congress finds the following:

(1) Information security technology, encryption, is—

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

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

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

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

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

(F) basic to the protection of the nation's critical infrastructures, including electrical grids, banking and financial systems, tele-

communications, water supplies, and transportation.

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

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

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

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

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

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

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

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

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

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

(12) A court order process should be required for access to plaintext, where and when available,

and criminal and civil penalties should be imposed for misuse of decryption information.

(13) Timely access to plaintext capability is—

(A) necessary to thwarting potential terrorist activities;

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

(C) indispensable to force protection requirements;

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

(E) both technically and economically possible.

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

(15) Unless law enforcement has the benefit of such market encouragement, drug traffickers, spies, child pornographers, pedophiles, kidnappers, terrorists, mobsters, weapons proliferators, fraud schemers, and other criminals will be able to use

encryption software to protect their criminal activity and hinder the criminal justice system.

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

TITLE I—DOMESTIC USES OF ENCRYPTION

SEC. 101. DEFINITIONS.

For purposes of this Act:

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

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

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

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

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

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

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

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

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

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

encrypting or decrypting any data, including communications.

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

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

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

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

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

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

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

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

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

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

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

(A) any citizen of the United States;

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

(C) any person organized under the laws of any foreign country who is owned or controlled

by individuals or persons described in subparagraphs (A) and (B).

SEC. 102. LAWFUL USE OF ENCRYPTION.

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

SEC. 103. UNLAWFUL USE OF ENCRYPTION.

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

"CHAPTER 125—ENCRYPTED DATA, INCLUDING COMMUNICATIONS

"Sec.
"2801. Unlawful use of encryption in furtherance of a criminal act.
"2802. Privacy protection.
"2803. Court order access to plaintext or decryption information.
"2804. Notification procedures.
"2805. Lawful use of plaintext or decryption information.
"2806. Identification of decryption information.
"2807. Definitions.

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

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

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

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

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

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

"§ 2802. Privacy protection

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

sponsible for providing the plaintext or the decryption information, pursuant to such order, to the investigative or law enforcement officer.

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

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

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

"(3) The court receiving such electronic or similar type of record described in paragraph (1) shall make the

original and a certified copy of the record available to the attorney for the Government making application under this section, and to the attorney for, or directly to, the owner of the data, including communications, who is the user of the encryption product, pursuant to the notification procedures set forth in section 2804.

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

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

"§ 2804. Notification procedures

"(a) IN GENERAL.—Within a reasonable time, but not later than 90 days after the filing of an application for an order under section 2803 which is granted, the court shall cause to be served, on the persons named in the order or the application, and such other parties whose

decryption information or whose plaintext has been provided to an investigative or law enforcement officer pursuant to this chapter, as the court may determine is in the interest of justice, an inventory which shall include notice of—

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Such motion shall be made before the trial, hearing, or proceeding unless there was no opportunity to make such motion, or the person was not aware of the grounds of the motion. If the motion is granted, the plaintext of the decrypted data, including communications, or evidence derived therefrom, shall be treated as having been obtained

in violation of this chapter. The court, upon the filing of such motion by the aggrieved person, may make available to the aggrieved person or that person's counsel for inspection such portions of the decrypted plaintext, or evidence derived therefrom, as the court determines to be in the interests of justice.

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

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

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

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

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

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

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

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

"(l) TECHNICAL ASSISTANCE BY PROVIDERS.—A provider of encryption technology or network service that has received an order issued by a court pursuant to this

chapter shall provide to the investigative or law enforcement officer concerned such technical assistance as is necessary to execute the order. Such provider may, however, move the court to modify or quash the order on the ground that its assistance with respect to the decryption or access to plaintext cannot be performed in fact, or in a timely or reasonable fashion. The court, upon notice to the Government, shall decide such motion expeditiously.

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

"§ 2805. Lawful use of plaintext or decryption information

"(a) AUTHORIZED USE OF DECRYPTION INFORMATION.—

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

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

"(b) LIMITATION.—An investigative or law enforcement officer may not use decryption information obtained under this chapter to determine the plaintext of any data,

including communications, unless it has obtained lawful authority to obtain such data, including communications, under other lawful authorities.

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

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

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

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

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

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

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

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

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

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

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

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

"(4) pursuant to a determination by a court of competent jurisdiction that another person is lawfully entitled to hold such decryption information, including determinations arising from legal pro-

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

"(5) otherwise permitted by law.

"§ 2806. Identification of decryption information

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

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

"§ 2807. Definitions

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

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

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

TITLE II—GOVERNMENT PROCUREMENT

SEC. 201. FEDERAL PURCHASES OF ENCRYPTION PRODUCTS.

(a) DECRYPTION CAPABILITIES.—The President may, consistent with the provisions of subsection (b), direct that any encryption product or service purchased or otherwise procured by the United States Government to provide the security service of data confidentiality for a computer system owned and operated by the United States Government shall include recoverability features or functions that enable the timely decryption of encrypted data, including communications, or timely access to plaintext by an authorized party without the knowledge or cooperation of the person using such encryption products or services.

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

SEC. 202. NETWORKS ESTABLISHED WITH FEDERAL FUNDS.

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

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

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

SEC. 203. GOVERNMENT CONTRACT AUTHORITY.

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

knowledge or cooperation of the person using such encryption products or services.

SEC. 204. PRODUCT LABELS.

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

SEC. 205. NO PRIVATE MANDATE.

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

SEC. 206. EXCLUSION.

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

TITLE III—EXPORTS OF ENCRYPTION

SEC. 301. EXPORTS OF ENCRYPTION.

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

(b) AUTHORITY TO DENY EXPORT FOR NATIONAL SECURITY REASONS.—Notwithstanding any provision of

this title, the President may deny the export of any encryption product on the basis that its export is contrary to the national security.

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

SEC. 302. LICENSE EXCEPTION FOR CERTAIN ENCRYPTION PRODUCTS.

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

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

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

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

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

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

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

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

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

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

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

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

(c) PERIODIC REVIEW OF LICENSE EXCEPTION ELIGIBILITY LEVEL.—(1) Not later than 180 days after the

date of the enactment of this Act, the President shall notify the Congress of the maximum level of encryption strength, which may not be lower than 64-bit, that may be exported from the United States under license exception pursuant to this section consistent with the national security.

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

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

SEC. 303. DISCRETIONARY AUTHORITY.

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

SEC. 304. EXPEDITED REVIEW AUTHORITY.

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

SEC. 305. ENCRYPTION LICENSES REQUIRED.

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

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

(A) gaining timely access to plaintext; or

(B) gaining timely access to decryption information.

(2) The export license applicant shall submit—

(A) the product for technical review;

(B) a certification, under oath, identifying—

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

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

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

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

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

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

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

(c) POST-EXPORT REPORTING.—

(1) UNAUTHORIZED USE.—All exporters of encryption products that are designed or manufactured within the United States shall submit a report to the Secretary at any time the exporter has reason

to believe any such exported product is being diverted to a use or a user not approved at the time of export.

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

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

(A) the particular product sold;

(B) the name and address of—

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

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

(C) the intended use of the product sold.

(d) EXERCISE OF OTHER AUTHORITIES.—The Secretary, the Secretary of Defense, and the Secretary of State may exercise the authorities they have under other provisions of law, including the Export Administration Act

of 1979, as continued in effect under the International Emergency Economic Powers Act, to carry out this title.

(e) WAIVER AUTHORITY.—

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

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

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

SEC. 306. ENCRYPTION INDUSTRY AND INFORMATION SECURITY BOARD.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(f) FINDINGS AND RECOMMENDATIONS.—The chair of the Board shall convey the findings and recommendations of the Board to the President and to the Congress within 30 days after each meeting of the Board. The rec-

ommendations of the Board are not binding upon the President.

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

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

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

TITLE IV—LIABILITY LIMITATIONS

SEC. 401. COMPLIANCE WITH COURT ORDER.

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

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

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

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

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

SEC. 402. COMPLIANCE DEFENSE.

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

SEC. 403. GOOD FAITH DEFENSE.

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

TITLE V—INTERNATIONAL AGREEMENTS

SEC. 501. SENSE OF CONGRESS.

It is the sense of Congress that—

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

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

SEC. 502. FAILURE TO NEGOTIATE.

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

SEC. 503. REPORT TO CONGRESS.

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

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

TITLE VI—MISCELLANEOUS PROVISIONS

SEC. 601. EFFECT ON LAW ENFORCEMENT ACTIVITIES.

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

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

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

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

SEC. 602. INTERPRETATION.

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

(1) preempt or otherwise affect the application of the Arms Export Control Act (22 U.S.C. 2751 et seq.), the Export Administration Act of 1979 (50 U.S.C. App. 2401 et seq.), or the International

Emergency Economic Powers Act (50 U.S.C. 1701 et seq.) or any regulations promulgated thereunder;

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

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

SEC. 603. FBI TECHNICAL SUPPORT.

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

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

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

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

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

SEC. 604. SEVERABILITY.

If any provision of this Act or the amendments made by this Act, or the application thereof, to any person or circumstances is held invalid by a court of the United States, the remainder of this Act or such amendments,

and the application thereof, to other persons or circumstances shall not be affected thereby.

○

Document No. 143