106TH CONGRESS
1st Session
HOUSE OF REPRESENTATIVES
REPT. 106–117
Part 2

SECURITY AND FREEDOM THROUGH ENCRYPTION (SAFE) ACT

JULY 2, 1999.—Ordered to be printed

Mr. BLILEY, from the Committee on Commerce, submitted the following

R E P O R T

[To accompany H.R. 850]

[Including cost estimate of the Congressional Budget Office]

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

CONTENTS

AMENDMENT

The amendment is as follows:

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

SECTION 1. SHORT TITLE.

This Act may be cited as the "Security And Freedom through Encryption (SAFE) Act".

SEC. 2. DEFINITIONS.

For purposes of this Act, the following definitions shall apply:

(1) COMPUTER HARDWARE.—The term "computer hardware" includes computer systems, equipment, application-specific assemblies, smart cards, modules, integrated circuits, printed circuit board assemblies, and devices that incorporate 1 or more microprocessor-based central processing units that are capable of accepting, storing, processing, or providing output of data.

(2) ENCRYPT AND ENCRYPTION.—The terms "encrypt" and "encryption" means the scrambling (and descrambling) of wire communications, electronic communications, or electronically stored information, using mathematical formulas or algorithms to preserve the confidentiality, integrity, or authenticity of, and prevent unauthorized recipients from accessing or altering, such communications or information.

(3) ENCRYPTION PRODUCT.—The term "encryption product"—

(A) means computer hardware, computer software, or technology with encryption capabilities; and

(B) includes any subsequent version of or update to an encryption product, if the encryption capabilities are not changed.

(4) KEY.—The term "key" means the variable information used in a mathematical formula, code, or algorithm, or any component thereof, used to decrypt wire communications, electronic communications, or electronically stored information, that has been encrypted.

(5) KEY RECOVERY INFORMATION.—The term "key recovery information" means information that would enable obtaining the key of a user of encryption.

(6) PERSON.—The term "person" has the meaning given the term in section 2510 of title 18, United States Code.

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

(8) STATE.—The term "State" means any State of the United States and includes the District of Columbia and any commonwealth, territory, or possessions of the United States.

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

(A) United States citizen; or

(B) legal entity that—

(i) is organized under the laws of the United States, or any States, the District of Columbia, or any commonwealth, territory, or possession of the United States; and

(ii) has its principal place of business in the United States.

(10) WIRE COMMUNICATION; ELECTRONIC COMMUNICATION.—The terms "wire communication" and "electronic communication" have the meanings given such terms in section 2510 of title 18, United States Code.

SEC. 3. ENSURING DEVELOPMENT AND DEPLOYMENT OF ENCRYPTION IS A VOLUNTARY PRIVATE SECTOR ACTIVITY.

(a) STATEMENT OF POLICY.—It is the policy of the United States that the use, development, manufacture, sale, distribution, and importation of encryption products, standards, and services for purposes of assuring the confidentiality, authenticity, or integrity of electronic information shall be voluntary and market driven.

(b) LIMITATION ON REGULATION.—Neither the Federal Government nor a State may establish any conditions, ties, or links between encryption products, standards, and services used for confidentiality, and those used for authenticity or integrity purposes.

SEC. 4. PROTECTION OF DOMESTIC SALE AND USE OF ENCRYPTION.

Except as otherwise provided by this Act, it is lawful for any person within any State, and for any United States person in a foreign country, to develop, manufacture, sell, distribute, import, or use any encryption product, regardless of the encryption algorithm selected, encryption key length chosen, existence of key recovery, or other plaintext access capability, or implementation or medium used.

SEC. 5. PROHIBITION ON MANDATORY GOVERNMENT ACCESS TO PLAINTEXT.

(a) IN GENERAL.—No department, agency, or instrumentality of the United States or of any State may require that, set standards for, condition any approval on, create incentives for, or tie any benefit to a requirement that, a decryption key, access to a key, key recovery information, or any other plaintext access capability be—

(1) required to be built into computer hardware or software for any purpose;

(2) given to any other person (including a department, agency, or instrumentality of the United States or an entity in the private sector that may be certified or approved by the United States or a State); or

(3) retained by the owner or user of an encryption key or any other person, other than for encryption products for the use of the United States Government or a State government.

(b) PROTECTION OF EXISTING ACCESS.—Subsection (a) does not affect the authority of any investigative or law enforcement officer, or any member of the intelligence community (as defined in section 3 of the National Security Act of 1947 (50 U.S.C. 401a)), acting under any law in effect on the date of the enactment of this Act, to gain access to encrypted communications or information.

SEC. 6. UNLAWFUL USE OF ENCRYPTION IN FURTHERANCE OF A CRIMINAL ACT.

(a) ENCRYPTION OF INCRIMINATING COMMUNICATIONS OR INFORMATION UNLAWFUL.—Any person who, in the commission of a felony under a criminal statute of the United States, knowingly and willfully encrypts incriminating communications or information relating to that felony with the intent to conceal such communications or information for the purpose of avoiding detection by law enforcement agencies or prosecution—

(1) in the case of a first offense under this section, shall be imprisoned for not more than 5 years, or fined under title 18, United States Code, or both; and

(2) in the case of a second or subsequent offense under this section, shall be imprisoned for not more than 10 years, or fined under title 18, United States Code, or both.

(b) USE OF ENCRYPTION NOT A BASIS FOR PROBABLE CAUSE.—The use of encryption by any person shall not be the sole basis for establishing probable cause with respect to a criminal offense or a search warrant.

SEC. 7. EXPORTS OF ENCRYPTION.

(a) AMENDMENT TO EXPORT ADMINISTRATION ACT OF 1979.—Section 17 of the Export Administration Act of 1979 (50 U.S.C. App. 2416) is amended by adding at the end the following new subsection:

"(g) CERTAIN CONSUMER PRODUCTS, COMPUTERS, AND RELATED EQUIPMENT.—

"(1) GENERAL RULE.—Subject to paragraphs (2), (3), and (4), the Secretary shall have exclusive authority to control exports of all computer hardware, software, computing devices, customer premises equipment, communications network equipment, and technology for information security (including encryption), except that which is specifically designed or modified for military use, including command, control, and intelligence applications.

"(2) CRITICAL INFRASTRUCTURE PROTECTION PRODUCTS.—

"(A) IDENTIFICATION.—Not later than 90 days after the date of the enactment of the Security And Freedom through Encryption (SAFE) Act, the Assistant Secretary of Commerce for Communications and Information and the National Telecommunications and Information Administration shall issue regulations that identify, define, or determine which products and equipment described in paragraph (1) are designed for improvement of network security, network reliability, or data security.

"(B) NTIA RESPONSIBILITY.—Not later than the expiration of the 2-year period beginning on the date of the enactment of the Security And Freedom through Encryption (SAFE) Act, all authority of the Secretary under this subsection and all determinations and reviews required by this section, with respect to products and equipment described in paragraph (1) that are designed for improvement of network security, network reliability, or data security through the use of encryption, shall be exercised through and made by the Assistant Secretary of Commerce for Communications and Information and the National Telecommunications and Information Administration. The Secretary may, at any time, assign to the Assistant Secretary and the NTIA authority of the Secretary under this section with respect to other products and equipment described in paragraph (1).

"(3) ITEMS NOT REQUIRING LICENSES.—After a one-time technical review by the Secretary of not more than 30 working days, which shall include consultation with the Secretary of Defense, the Secretary of State, the Attorney General, and the Director of Central Intelligence, no export license may be required, except pursuant to the Trading with the Enemy Act or the International Emergency Economic Powers Act (but only to the extent that the authority of such Act is not exercised to extend controls imposed under this Act), for the export or reexport of—

"(A) any computer hardware or software or computing device, including computer hardware or software or computing devices with encryption capabilities—

"(i) that is generally available;

"(ii) that is in the public domain for which copyright or other protection is not available under title 17, United States Code, or that is available to the public because it is generally accessible to the interested public in any form; or

"(iii) that is used in a commercial, off-the-shelf, consumer product or any component or subassembly designed for use in such a consumer product available within the United States or abroad which—

"(I) includes encryption capabilities which are inaccessible to the end user; and

"(II) is not designed for military or intelligence end use;

"(B) any computing device solely because it incorporates or employs in any form—

"(i) computer hardware or software (including computer hardware or software with encryption capabilities) that is exempted from any requirement for a license under subparagraph (A); or

"(ii) computer hardware or software that is no more technically complex in its encryption capabilities than computer hardware or software that is exempted from any requirement for a license under subparagraph (A) but is not designed for installation by the purchaser;

"(C) any computer hardware or software or computing device solely on the basis that it incorporates or employs in any form interface mechanisms for interaction with other computer hardware or software or computing devices, including computer hardware and software and computing devices with encryption capabilities;

"(D) any computing or telecommunication device which incorporates or employs in any form computer hardware or software encryption capabilities which—

"(i) are not directly available to the end user; or

"(ii) limit the encryption to be point-to-point from the user to a central communications point or link and does not enable end-to-end user encryption;

"(E) technical assistance and technical data used for the installation or maintenance of computer hardware or software or computing devices with encryption capabilities covered under this subsection; or

"(F) any encryption hardware or software or computing device not used for confidentiality purposes, such as authentication, integrity, electronic signatures, nonrepudiation, or copy protection.

"(4) COMPUTER HARDWARE OR SOFTWARE OR COMPUTING DEVICES WITH ENCRYPTION CAPABILITIES.—After a one-time technical review by the Secretary of not more than 30 working days, which shall include consultation with the Secretary of Defense, the Secretary of State, the Attorney General, and the Director of Central Intelligence, the Secretary shall authorize the export or reexport of computer hardware or software or computing devices with encryption capabilities for nonmilitary end uses in any country—

"(A) to which exports of computer hardware or software or computing devices of comparable strength are permitted for use by financial institutions not controlled in fact by United States persons, unless there is substantial evidence that such computer hardware or software or computing devices will be—

"(i) diverted to a military end use or an end use supporting international terrorism;

"(ii) modified for military or terrorist end use;

"(iii) reexported without any authorization by the United States that may be required under this Act; or

"(iv)(I) harmful to the national security of the United States, including capabilities of the United States in fighting drug trafficking, terrorism, or espionage, (II) used in illegal activities involving the sexual exploitation of, abuse of, or sexually explicit conduct with minors (including activities in violation of chapter 110 of title 18, United States Code, and section 2423 of such title), or (III) used in illegal activities involving organized crime; or

"(B) if the Secretary determines that a computer hardware or software or computing device offering comparable security is commercially available in such country from a foreign supplier, without effective restrictions.

"(5) DEFINITIONS.—For purposes of this subsection—

"(A) the term 'computer hardware' has the meaning given such term in section 2 of the Security And Freedom through Encryption (SAFE) Act;

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

"(C) the term 'customer premises equipment' means equipment employed on the premises of a person to originate, route, or terminate communications;

"(D) the term 'data security' means the protection, through techniques used by individual computer and communications users, of data from unauthorized penetration, manipulation, or disclosure;

"(E) the term 'encryption' has the meaning given such term in section 2 of the Security And Freedom through Encryption (SAFE) Act;

"(F) the term 'generally available' means, in the case of computer hardware or computer software (including computer hardware or computer software with encryption capabilities)—

"(i) computer hardware or computer software that is—

"(I) distributed through the Internet;

"(II) offered for sale, license, or transfer to any person without restriction, whether or not for consideration, including, but not limited to, over-the-counter retail sales, mail order transactions, phone order transactions, electronic distribution, or sale on approval;

"(III) preloaded on computer hardware or computing devices that are widely available for sale to the public; or

"(IV) assembled from computer hardware or computer software components that are widely available for sale to the public;

"(ii) not designed, developed, or tailored by the manufacturer for specific purchasers or users, except that any such purchaser or user may—

"(I) supply certain installation parameters needed by the computer hardware or software to function properly with the computer system of the user or purchaser; or

"(II) select from among options contained in the computer hardware or computer software; and

"(iii) with respect to which the manufacturer of that computer hardware or computer software—

"(I) intended for the user or purchaser, including any licensee or transferee, to install the computer hardware or software and has supplied the necessary instructions to do so, except that the manufacturer of the computer hardware or software, or any agent of such manufacturer, may also provide telephone or electronic mail help line services for installation, electronic transmission, or basic operations; and

"(II) the computer hardware or software is designed for such installation by the user or purchaser without further substantial support by the manufacturer;

"(G) the term 'network reliability' means the prevention, through techniques used by providers of computer and communications services, of the malfunction, and the promotion of the continued operations, of computer or communications network;

"(H) the term 'network security' means the prevention, through techniques used by providers of computer and communications services, of unauthorized penetration, manipulation, or disclosure of information of a computer or communications network;

"(I) the term 'technical assistance' includes instruction, skills training, working knowledge, consulting services, and the transfer of technical data;

"(J) the term 'technical data' includes blueprints, plans, diagrams, models, formulas, tables, engineering designs and specifications, and manuals and instructions written or recorded on other media or devices such as disks, tapes, or read-only memories; and

"(K) the term 'technical review' means a review by the Secretary of computer hardware or software or computing devices with encryption capabilities, based on information about the product's encryption capabilities supplied by the manufacturer, that the computer hardware or software or computing device works as represented.".

(b) TRANSFER OF AUTHORITY TO NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION.—Section 103(b) of the National Telecommunications and In-

formation Administration Organization Act (47 U.S.C. 902(b)) is amended by adding at the end the following new paragraph:

"(4) EXPORT OF COMMUNICATIONS TRANSACTION TECHNOLOGIES.—In accordance with section 17(g)(2) of the Export Administration Act of 1979 (50 U.S.C. App. 2416(g)(2)), the Secretary shall assign to the Assistant Secretary and the NTIA the authority of the Secretary under such section 17(g), with respect to products and equipment described in paragraph (1) of such section that are designed for improvement of network security, network reliability, or data security, that (after the expiration of the 2-year period beginning on the date of the enactment of the Security And Freedom through Encryption (SAFE) Act) is to be exercised by the Assistant Secretary and the NTIA.".

(c) NO REINSTATEMENT OF EXPORT CONTROLS ON PREVIOUSLY DECONTROLLED PRODUCTS.—Any encryption product not requiring an export license as of the date of enactment of this Act, as a result of administrative decision or rulemaking, shall not require an export license on or after such date of enactment.

(d) APPLICABILITY OF CERTAIN EXPORT CONTROLS.—

(1) IN GENERAL.—Nothing in this Act shall limit the authority of the President under the International Emergency Economic Powers Act, the Trading with the Enemy Act, or the Export Administration Act of 1979, to—

(A) prohibit the export of encryption products to countries that have been determined to repeatedly provide support for acts of international terrorism; or

(B) impose an embargo on exports to, and imports from, a specific country.

(2) SPECIFIC DENIALS.—The Secretary of Commerce may prohibit the export of specific encryption products to an individual or organization in a specific foreign country identified by the Secretary, if the Secretary determines that there is substantial evidence that such encryption products will be—

(A) used for military or terrorist end-use or modified for military or terrorist end use;

(B) harmful to United States national security, including United States capabilities in fighting drug trafficking, terrorism, or espionage;

(C) used in illegal activities involving the sexual exploitation of, abuse of, or sexually explicit conduct with minors (including activities in violation of chapter 110 of title 18, United States Code, and section 2423 of such title); or

(D) used in illegal activities involving organized crime.

(3) OTHER EXPORT CONTROLS.—An encryption product is subject to any export control imposed on that product for any reason other than the existence of encryption capability. Nothing in this Act or the amendments made by this Act alters the ability of the Secretary of Commerce to control exports of products for reasons other than encryption.

(e) CONTINUATION OF EXPORT ADMINISTRATION ACT.—For purposes of carrying out the amendment made by subsection (a), the Export Administration Act of 1979 shall be deemed to be in effect.

SEC. 8. GOVERNMENT PROCUREMENT OF ENCRYPTION PRODUCTS.

(a) STATEMENT OF POLICY.—It is the policy of the United States—

(1) to permit the public to interact with government through commercial networks and infrastructure; and

(2) to protect the privacy and security of any electronic communication from, or stored information obtained from, the public.

(b) PURCHASE OF ENCRYPTION PRODUCTS BY FEDERAL GOVERNMENT.—Any department, agency, or instrumentality of the United States may purchase encryption products for internal use by officers and employees of the United States to the extent and in the manner authorized by law.

(c) PROHIBITION OF REQUIREMENT FOR CITIZENS TO PURCHASE SPECIFIED PRODUCTS.—No department, agency, or instrumentality of the United States, nor any department, agency, or political subdivision of a State, may require any person in the private sector to use any particular encryption product or methodology, including products with a decryption key, access to a key, key recovery information, or any other plaintext access capability, to communicate with, or transact business with, the government.

SEC. 9. NATIONAL ELECTRONIC TECHNOLOGIES CENTER.

Part A of the National Telecommunications and Information Administration Organization Act is amended by inserting after section 105 (47 U.S.C. 904) the following new section:

"SEC. 106. NATIONAL ELECTRONIC TECHNOLOGIES CENTER.

"(a) ESTABLISHMENT.—There is established in the NTIA a National Electronic Technologies Center (in this section referred to as the 'NET Center').

"(b) DIRECTOR.—The NET Center shall have a Director, who shall be appointed by the Assistant Secretary.

"(c) DUTIES.—The duties of the NET Center shall be—

"(1) to serve as a center for industry and government entities to exchange information and methodology regarding data security techniques and technologies;

"(2) to examine encryption techniques and methods to facilitate the ability of law enforcement to gain efficient access to plaintext of communications and electronic information;

"(3) to conduct research to develop efficient methods, and improve the efficiency of existing methods, of accessing plaintext of communications and electronic information;

"(4) to investigate and research new and emerging techniques and technologies to facilitate access to communications and electronic information, including —

"(A) reverse-steganography;

"(B) decompression of information that previously has been compressed for transmission; and

"(C) de-multiplexing;

"(5) to obtain information regarding the most current computer hardware and software, telecommunications, and other capabilities to understand how to access information transmitted across computer and communications networks; and

"(6) to serve as a center for Federal, State, and local law enforcement authorities for information and assistance regarding decryption and other access requirements.

"(d) EQUAL ACCESS.—State and local law enforcement agencies and authorities shall have access to information, services, resources, and assistance provided by the NET Center to the same extent that Federal law enforcement agencies and authorities have such access.

"(e) PERSONNEL.—The Director may appoint such personnel as the Director considers appropriate to carry out the duties of the NET Center.

"(f) ASSISTANCE OF OTHER FEDERAL AGENCIES.—Upon the request of the Director of the NET Center, the head of any department or agency of the Federal Government may, to assist the NET Center in carrying out its duties under this section—

"(1) detail, on a reimbursable basis, any of the personnel of such department or agency to the NET Center; and

"(2) provide to the NET Center facilities, information, and other non-personnel resources.

"(g) PRIVATE INDUSTRY ASSISTANCE.—The NET Center may accept, use, and dispose of gifts, bequests, or devises of money, services, or property, both real and personal, for the purpose of aiding or facilitating the work of the Center. Gifts, bequests, or devises of money and proceeds from sales of other property received as gifts, bequests, or devises shall be deposited in the Treasury and shall be available for disbursement upon order of the Director of the NET Center.

"(h) ADVISORY BOARD.—

"(1) ESTABLISHMENT.—There is established the Advisory Board of the NET Center (in this subsection referred to as the "Advisory Board"), which shall be comprised of 11 members who shall have the qualifications described in paragraph (2) and who shall be appointed by the Assistant Secretary not later than 6 months after the date of the enactment of this Act. The chairman of the Advisory Board shall be designated by the Assistant Secretary at the time of appointment.

"(2) QUALIFICATIONS.—Each member of the Advisory Board shall have experience or expertise in the field of encryption, decryption, electronic communication, information security, electronic commerce, or law enforcement.

"(3) DUTIES.—The duty of the Advisory Board shall be to advise the NET Center and the Federal Government regarding new and emerging technologies relating to encryption and decryption of communications and electronic information.

"(i) IMPLEMENTATION PLAN.—Within 2 months after the date of the enactment of this Act, the Assistant Secretary, in consultation and cooperation with other appropriate Federal agencies and appropriate industry participants, develop and cause to be published in the Federal Register a plan for establishing the NET Center. The plan shall—

"(1) specify the physical location of the NET Center and the equipment, software, and personnel resources necessary to carry out the duties of the NET Center under this section;

"(2) assess the amount of funding necessary to establish and operate the NET Center; and

"(3) identify sources of probable funding for the NET Center, including any sources of in-kind contributions from private industry.".

SEC. 10. STUDY OF NETWORK AND DATA SECURITY ISSUES.

Part C of the National Telecommunications and Information Administration Organization Act is amended by adding at the end the following new section:

"SEC. 156. STUDY OF NETWORK RELIABILITY AND SECURITY AND DATA SECURITY ISSUES.

"(a) IN GENERAL.—The NTIA shall conduct an examination of—

"(1) the relationship between—

"(A) network reliability (for communications and computer networks), network security (for such networks), and data security issues; and

"(B) the conduct, in interstate commerce, of electronic commerce transactions, including through the medium of the telecommunications networks, the Internet, or other interactive computer systems;

"(2) the availability of various methods for encrypting communications; and

"(3) the effects of various methods of providing access to encrypted communications and to information to further law enforcement activities.

"(b) SPECIFIC ISSUES.—In conducting the examination required by subsection (a), the NTIA shall—

"(1) analyze and evaluate the requirements under paragraphs (3) and (4) of section 17(g) of the Export Administration Act of 1979 (50 U.S.C. App. 2416(g); as added by section 7(a) of this Act) for products referred to in such paragraphs to qualify for the license exemption or mandatory export authorization under such paragraphs, and determine—

"(A) the scope and applicability of such requirements and the products that, at the time of the examination, qualify for such license exemption or export authorization; and

"(B) the products that will, 12 months after the examination is conducted, qualify for such license exemption or export authorization; and

"(2) assess possible methods for providing access to encrypted communications and to information to further law enforcement activities.

"(c) REPORTS.—Within one year after the date of enactment of this section, the NTIA shall submit to the Congress and the President a detailed report on the examination required by subsections (a) and (b). Annually thereafter, the NTIA shall submit to the Congress and the President an update on such report.

"(d) DEFINITIONS.—For purposes of this section—

"(1) the terms 'data security', 'encryption', 'network reliability', and 'network security' have the meanings given such terms in section 17(g)(5) of the Export Administration Act of 1979 (50 U.S.C. App. 2416(g)(5)); and

"(2) the terms 'Internet' and 'interactive computer systems' have the meanings provided by section 230(e) of the Communications Act of 1934 (47 U.S.C. 230(e)).".

SEC. 11. TREATMENT OF ENCRYPTION IN INTERSTATE AND FOREIGN COMMERCE.

(a) INQUIRY REGARDING IMPEDIMENTS TO COMMERCE.—Within 180 days after the date of the enactment of this Act, the Secretary of Commerce shall complete an inquiry to—

(1) identify any domestic and foreign impediments to trade in encryption products and services and the manners in which and extent to which such impediments inhibit the development of interstate and foreign commerce; and

(2) identify import restrictions imposed by foreign nations that constitute trade barriers to providers of encryption products or services.

The Secretary shall submit a report to the Congress regarding the results of such inquiry by such date.

(b) REMOVAL OF IMPEDIMENTS TO TRADE.—Within 1 year after such date of enactment, the Secretary shall prescribe such regulations as may be necessary to reduce the impediments to trade in encryption products and services identified in the inquiry pursuant to subsection (a) for the purpose of facilitating the development of interstate and foreign commerce. Such regulations shall be designed to—

(1) promote the sale and distribution, including through electronic commerce, in foreign commerce of encryption products and services manufactured in the United States; and

(2) strengthen the competitiveness of domestic providers of encryption products and services in foreign commerce, including electronic commerce.

(c) INTERNATIONAL AGREEMENTS.—

(1) REPORT TO PRESIDENT.—Upon the completion of the inquiry under subsection (a), the Secretary shall submit a report to the President regarding reducing any impediments to trade in encryption products and services that are identified by the inquiry and could, in the determination of the Secretary, require international negotiations for such reduction.

(2) NEGOTIATIONS.—The President shall take all actions necessary to conduct negotiations with other countries for the purposes of (A) concluding international agreements on the promotion of encryption products and services, and (B) achieving mutual recognition of countries' export controls, in order to meet the needs of countries to preserve national security, safeguard privacy, and prevent commercial espionage. The President may consider a country's refusal to negotiate such international export and mutual recognition agreements when considering the participation of the United States in any cooperation or assistance program with that country. The President shall submit a report to the Congress regarding the status of international efforts regarding cryptography not later than December 31, 2000.

SEC. 12. COLLECTION OF INFORMATION ON EFFECT OF ENCRYPTION 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 (as defined in section 2801 of title 18, United States Code) 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. 13. PROHIBITION ON TRANSFERS TO PLA AND COMMUNIST CHINESE MILITARY COMPANIES.

(a) PROHIBITION.—Whoever knowingly and willfully transfers to the People's Liberation Army or to any Communist Chinese military company any encryption product that utilizes a key length of more than 56 bits—

(1) in the case of a first offense under this section, shall be imprisoned for not more than 5 years, or fined under title 18, United States Code, or both; and

(2) in the case of second or subsequent offense under this section, shall be imprisoned for not more than 10 years, or fined under title 18, United States Code, or both.

(b) DEFINITIONS.—For purposes of this section:

(1) COMMUNIST CHINESE MILITARY COMPANY.—(A) Subject to subparagraph (B), the term "Communist Chinese military company" has the meaning given that term in section 1237(b)(4) of the Strom Thurmond National Defense Authorization Act for Fiscal Year 1999 (50 U.S.C. 1701 note).

(B) At such time as the determination and publication of persons are made under section 1237(b)(1) of the Strom Thurmond National Defense Authorization Act for Fiscal Year 1999, the term "Communist Chinese military company" shall mean the list of those persons so published, as revised under section 1237(b)(2) of that Act.

(2) PEOPLE'S LIBERATION ARMY.—The term "People's Liberation Army" has the meaning given that term in section 1237(c) of the Strom Thurmond National Defense Authorization Act for Fiscal Year 1999.

SEC. 14. FAILURE TO DECRYPT INFORMATION OBTAINED UNDER COURT ORDER.

Whoever is required by an order of any court to provide to the court or any other party any information in such person's possession which has been encrypted and who, having possession of the key or such other capability to decrypt such information into the readable or comprehensible format of such information prior to its encryption, fails to provide such information in accordance with the order in such readable or comprehensible form—

(1) in the case of a first offense under this section, shall be imprisoned for not more than 5 years, or fined under title 18, United States Code, or both; and

(2) in the case of second or subsequent offense under this section, shall be imprisoned for not more than 10 years, or fined under title 18 United States Code, or both.

PURPOSE AND SUMMARY

H.R. 850, the Security And Freedom through Encryption (SAFE) Act, modernizes the encryption policy of the United States. It also addresses law enforcement and national security needs as strong encryption products become more widely used.

In summary, H.R. 850, as amended by the Committee on Commerce, clarifies U.S. policy regarding the domestic use of encryption products, including prohibiting the Federal government or State governments from requiring key recovery or a similar technique in most circumstances and adding criminal penalties for the use of encryption products in the cover-up of felonious activity. H.R. 850 also relaxes U.S. export policies by permitting mass-market encryption products to be exported under a general license exception. It also permits other custom made computer hardware and software encryption products to be exported on an expedited basis. The bill includes a specified role for the National Telecommunications and Information Administration (NTIA) in the consideration of the export of certain encryption products.

H.R. 850 establishes a National Electronic Technologies Center (NET Center) to help Federal, State, and local law enforcement agencies obtain access to encrypted communications. The Center will aid law enforcement in accessing encrypted communications and information by promoting a positive relationship with the related industry.

H.R. 850 also requires: an annual in-depth analysis of the relationship between network reliability, network security, and data security and the conduct of transactions in interstate commerce; an examination of foreign barriers to the importation of U.S. encryption products and positive steps to be taken to remove these barriers; and that the Attorney General compile information regarding instances when law enforcement's efforts have been stymied because of the use of strong encryption products. The information from these efforts will be helpful in analyzing the impact of increased use of encryption products.

BACKGROUND AND NEED FOR LEGISLATION

I. Background

Encryption is the commonly used term to describe the use of cryptography to ensure the confidentiality of messages. Encryption products can be either computer software or hardware and can be used over any electronic medium (e.g., the public switched telephone network, or the Internet). The strength of an encryption product, and thus the likelihood that a message will remain confidential as it travels through a network, is measured in terms of bits. For example, a two-bit code results in four possible combinations of messages (00, 01, 10, 11), whereas a 56-bit code results in millions of possible combinations. "Keys" are widely used in today's encryption technology to encrypt/decrypt messages. While encrypting messages was historically the province of the military, the growing use of computers on both public and private networks has led to development of new commercially available products designed for non-military purposes. For instance, the use of encryption products can be an effective mechanism to promote the

reliability of the telecommunications networks and to secure data related to electronic commerce transactions.

A. Current law and regulation

Current law generally prohibits the export of certain controlled encryption products. Such products can be exported if they qualify for a license exception or the exporter obtains individual licenses, which means approval by the reviewing agency. Federal restrictions generally prohibit the export of encryption products that are above a specified level of strength (e.g., 56-bit length). Federal law currently imposes no import or domestic restrictions on encryption products (i.e., encryption products of any strength are available for domestic use, regardless of whether the product is developed here or abroad). These export restrictions are intended to ensure strong U.S. encryption products do not fall into the hands of countries where the intelligence community is gathering information, terrorists, or rogue countries.

The Administration has modified its encryption policy a number of times over the course of the last several years. For instance, U.S. encryption policy was amended in December 1996 to permit the export of encryption products of any length to financial institutions. The Administration reviews and, if necessary revises, its encryption products policy every six months. The Department of Commerce's current encryption products rules (modified as recently as December 31, 1998) can be generally summarized as follows:

(1) there are no restrictions on the ability to buy, sell, manufacture, or distribute encryption products within the United States;

(2) 56-bit (or lower) encryption products, without being recoverable, may be exported after a one-time review;

(3) encryption products above 56 bits for use by subsidiaries of American companies for the protection of international business can be exported under a license exemption, except to the seven terrorist nations;

(4) encryption products above 56 bits can be exported under a license exception or a license exception-like treatment and can be exported to 45 specified countries for use by the health and medical companies, insurance companies, and online merchants; and

(5) encryption products above 56 bits for use by foreign commercial firms for internal company proprietary use may be exported to specified countries under licensing exception treatment—only if the manufacturer provides a "recoverable mechanism" that allows for the recovery of plaintext.

B. International developments

While a number of countries have export or import restrictions on encryption products, those that do often do not have rules as stringent as the United States' rules. The Clinton Administration has been negotiating with Member countries of the "Wassenaar Arrangement" to develop a unified approach to rules relating to the export of encryption products. The Wassenaar Arrangement was created in 1996 as a global multilateral arrangement on export controls for conventional weapons and sensitive dual-use goods and

technologies. In December 1998, the Administration announced that the participating countries reached agreement to impose export restrictions for certain encryption products. The 33 signatories represent a large portion of the countries producing encryption products.

C. Recent litigation

On May 6, 1999, the United States Court of Appeals for the Ninth Circuit rendered a decision in *Bernstein* v. *United States*, No. 97–16686, 1999 U.S. App. Lexis 8595 (9th Cir. 1999). Professor Daniel Bernstein filed suit against the Federal government after he was notified by the State Department that his "Snuffle" encryption program would require an export license to post the source code on the Internet. In a 2–1 decision, the Ninth Circuit upheld the trial court's ruling that the regulation of Bernstein's export of his encryption program constituted an impermissible prior restraint on speech. The Administration has not decided whether it will appeal the Ninth Circuit's ruling.

In addition, in *Karn* v. *Dept. of State*, 925 F.Supp. 1 (D.D.C. 1996), remanded, 1997 U.S. App. Lexis 3123 (D.C. Cir. 1997), the District Court for the District of Columbia ruled that the export restrictions were not subject to judicial review, but do not violate the First Amendment.

II. Arguments in the debate over encryption products

The debate over the export of encryption products centers around whether: (1) U.S. companies should be permitted to export encryption products of any strength, thus increasing the availability of such products in the global market; and (2) there should be restrictions on use of encryption products within the United States. In general, sound encryption policy must balance privacy interests with society's interest in protecting the public. To the greatest extent possible, it must also be based on free-market principles.

The high technology industry and the business community argue that current U.S. encryption policy harms domestic businesses with operations abroad because they are forced to export weak encryption products that compete with stronger foreign encryption products. These technology builders and users point out that today's informal world standard that encryption users demand is based on encryption products with 128 bit technology. However, under the Administration's current policy, encryption products, based on 56 bit technology, are exportable without restriction while encryption products above this level are subject to significant export limitations.

The high technology industry and business community also argue that the current policy has a direct impact on the strength of encryption products available within the United States. In practice, current U.S. encryption policy, while based on export restrictions acts as a de facto domestic restriction for U.S. encryption manufacturers. American firms are either unwilling or unable to spend the resources to develop two products—one available for domestic use, and another less robust product that may be exported. Instead,

American firms develop one product at the lowest level of encryption to comply with the more stringent export laws.

Many representatives of the high technology and business community also argue that the security of a strong encryption product is jeopardized if it contains a recoverable feature. They claim that recoverable products contain a larger number of flaws and weaknesses in encryption products, which can be exploited by unauthorized people to gain entry to secure communications or information. Further, they argue that the regime necessary for recoverable products to operate (e.g., key management) increases the likelihood of implementation and management problems that can weaken the effectiveness of encryption products. Therefore, they conclude that stronger, non-recoverable products effectively help to prevent crime.

In addition, the high technology industry generally argues that the current policy may impose excessive costs as they may be forced to develop prohibitively costly, new recoverable products; manufacture two different products (one for the domestic use (strong) and one for abroad (weaker)); and/or be subject to a burdensome licensing process. Therefore, U.S. domestic manufacturers argue that the United States is losing market share to foreign software and hardware firms, which face fewer restrictions.

Alternatively, government officials, which include Federal, State, and local law enforcement officials, argue that permitting the export of stronger encryption products without a clear mechanism to decrypt a communication or stored information, when necessary and lawful, will jeopardize public safety and national security. They believe that recoverable encryption products must be developed, not only to facilitate lawful searches and seizures, but to help users or employers in the event they lose the ability to decrypt a communications or related information. They also argue that widespread use of strong encryption without being recoverable would infringe on their surveillance techniques.

In addition, the national security community argues that most foreign countries view lifting the export restrictions as America's attempt to dominate world markets at the expense of other nations' national security, thereby forcing these countries to adopt import restrictions to keep American products out of their countries. Further, they point out that official government access to sensitive international communications (e.g., e-mail traffic between terrorist groups and manufacturing operations) will be stopped or curtailed if strong encryption products are allowed to proliferate. They argue that since U.S. encryption products are the most influential and dominant in the marketplace, limiting or implementing a policy of containment (i.e., preventing or limiting the spread and use of strong encryption products) of U.S.-made encryption products is necessary for the national security community to continue to do its job. Loosening of encryption rules, they note, would also impair the ability of our intelligence agencies to track the use of strong U.S. encryption products overseas since removing export controls would also remove complementary reporting requirements.

Lastly, both law enforcement and national security communities point out that the current policy is flexible enough to allow the export of strong encryption products. These groups further contend

that the current policy is under constant review and will change based on new information regarding encryption products or changes in technology.

III. Need for encryption products policy reform

Electronic commerce, the growth in use of the Internet, and the innovation of U.S. high technology companies are helping drive the economic prosperity experienced today in the U.S. and worldwide. In sum, the world is in the early stages of the formation of the digital age. However, barriers remain to the full development of these capabilities and underlying transaction mediums. Today, consumer wariness over the safety, security, and privacy of information transmitted via electronic mediums has been listed very often in consumer surveys as a reason more consumers are not utilizing these technologies.

Encryption and the prolific use of encryption products are essential to ease consumers' worries about the availability of their sensitive information to unwanted parties. Unfortunately, the Administration's existing policy towards the export of U.S. manufactured encryption products is hampering the use of such technology. Existing U.S. encryption policy is partly premised upon the belief that minimizing the proliferation of U.S. manufactured encryption products worldwide will minimize the use of encryption products overall. Thus, current U.S. encryption policy is based upon the theory of containment rather than access.

The Committee is not convinced that reliance on export restrictions provides adequate assistance to national security personnel in their ever increasing need to keep up with the latest technologies. The Committee finds that the current export rules place domestic manufacturers of encryption products at a competitive disadvantage with respect to their foreign counterparts. Moreover, bad actors simply use strong encryption products manufactured by foreign producers. Containment, which is the heart of the national security argument, prevents U.S. manufacturers from exporting strong encryption products to serve international and U.S. customers, while allowing foreign encryption manufacturers that abide by lesser restrictions an inherent, unfair market advantage.

While it may be possible that the containment strategy may be slowing the proliferation of strong encryption products, it is not stopping its proliferation and will not do so as technology becomes more prevalent and consumers' demand for security and privacy increases. Foreign strong encryption products are turning up not only in the hands of international criminals and rogue agents, but also are being used by U.S.-based multi-national companies within the U.S. borders in order to provide the necessary security strong encryption products users can afford. Thus, current export restrictions are effective in containing our domestic encryption manufacturers.

The containment aspect of current policy is also flawed by its lack of uniformity and consistency. To be more effective and to further the goal of containing strong encryption products, it would be expected that the Administration would also favor import restrictions to prevent foreign encryption products manufacturers from importing strong encryption products into the United States. The

United States is by far the largest single marketplace of high technology users. However, as the use of strong encryption products becomes more prevalent, it becomes increasingly difficult to contain them within U.S. borders. Current policy does not advocate (nor would the Committee favor) import restrictions. The lack of an import regime makes the containment component of the current policy highly questionable.

Current encryption policy is also based on providing law enforcement officials access to encrypted communications and information through the voluntary promotion of recoverable products. Clearly, the needs of law enforcement are not being met by changes in technology. The Fourth Amendment and title III of the Omnibus Crime Control and Safe Streets Act of 1968 permit law enforcement agencies to search, seize, and intercept electronic communications and stored data. With the development of strong encryption technologies, however, law enforcement's efforts are being thwarted because even though they can search, seize, or intercept the information, they cannot understand it because it is encoded. Without the necessary tools, law enforcement does not have the ability to prevent and solve crimes. Thus, the law enforcement community seeks to promote the development and use of recoverable products by all parties. In their view, recoverable products can satisfy both demand for strong encryption products and law enforcement's need to access such underlying communications or information under proper authority.

The Committee finds the current encryption policy is fundamentally flawed in its goal to promote the voluntary use of recoverable encryption. For instance, current policy allows the export of strong encryption products to certain market segments for certain countries—covering over 70 percent of all business activity according to the Administration. The current policy permits and even touts that recoverable features are not necessary for a large portion of encryption products. Thus, while law enforcement would like recoverable features to be built into all encryption products, the current policy, which was developed with the law enforcement community's involvement, does not include such a requirement.

While certain recoverable encryption products are allowed to be exported today, it is not necessarily the current policy that has led to this result. Instead, some companies are seeking permission to export some recoverable products for certain uses because the marketplace, more specifically, the end-users, demand such capabilities. However, the evidence before the Committee strongly suggests that recoverable products are not currently in demand. Computer users, for the most part, do not support having back-door access built into their encryption products. Thus, current policy cannot and should not continue to be based on allowing recoverable products favorable treatment under the export regime.

Consequently, the Committee has turned to the legislative process to provide a sound policy for the export of encryption products. The policy contained in H.R. 850, as reported by the Committee on Commerce, addresses the needs of law enforcement to access encrypted communications while easing existing export restrictions that hamper domestic manufacturers of encryption products.

As reported by the Committee on Commerce, H.R. 850 takes a significant step towards addressing the concerns of law enforcement. The legislation creates a "National Electronic Technologies Center" (NET Center) that will assemble experts on encryption technology to develop and advise law enforcement officials on how to access encrypted electronic communications or information. The NET Center also will look ahead to future technologies and assist law enforcement with decryption techniques as new technologies are introduced. The Committee concludes that a partnership between the industry and law enforcement is an appropriate means to help law enforcement protect public safety. The Committee also believes that this approach will provide for increased access to encrypted communications and information.

The bill, as reported by the Committee, also addresses the needs of domestic manufacturers of encryption products by granting export relief for certain encryption products. This change in export policy should place the U.S. high technology industry in a position where domestic companies producing encryption products can compete on a level playing field with their competitors in a global market. Moreover, H.R. 850 seeks to push for further relief for U.S. manufacturers by directing the Department of Commerce to reduce foreign impediments to trade.

H.R. 850 also codifies current policy regarding the availability and use of encryption products within the U.S. The Committee has great interest in making sure that the current policy, which does not restrict the legitimate use of encryption products within the U.S., does not change.

On process, the Administration argues that there is no need for legislation on this matter because current policy allows for more flexible regulation updates than allowed for under H.R. 850. This perspective, however, ignores or overlooks two very important respects. First, while revising current export restrictions through modification of Federal regulations is possible, the Administration has shown little interest, beyond certain strong rhetoric, in providing the significant export relief contemplated by H.R. 850. Thus, while altering current regulations could be a faster mechanism to change policy than legislation, there is no evidence that the Administration will make such changes any time soon. Further, the approach contained in section 7 of H.R. 850, as reported by the Committee (basing the permissible export of encryption products by U.S. companies on the availability of encryption products already in the market), provides significant and sufficient flexibility to respond to the changing marketplace for encryption products.

Overall, the Committee finds that H.R. 850, as reported, strikes the appropriate balance between the needs of law enforcement and those of the U.S. high technology industry and business community.

HEARINGS

The Subcommittee on Telecommunications, Trade, and Consumer Protection held a legislative hearing on H.R. 850, the Security And Freedom through Encryption (SAFE) Act, on May 25, 1999. The Subcommittee received testimony from: The Honorable William A. Reinsch, Undersecretary of Commerce for Export Administration,

United States Department of Commerce; The Honorable Ronald D. Lee, Associate Deputy Attorney General, United States Department of Justice; The Honorable Barbara A. McNamara, Deputy Director, National Security Agency; Mr. David D. Dawson, Chairman and CEO, V–ONE Corporation; Mr. Paddy Holahan, Executive Vice President of Marketing, Baltimore Technologies; Mr. Richard Hornstein, Vice President of Legal Affairs, Taxation, and Corporate Development, Network Associates, on behalf of the Business Software Alliance; Mr. Tom Arnold, Vice President & Chief Technology Officer, CyberSource Corp.; Dr. E. Eugene Schultz, Ph.D., CISSP, Trusted Security Advisor and Research Director, Global Integrity Corporation; and Mr. Ed Gillespie, Executive Director, Americans for Computer Privacy (ACP).

COMMITTEE CONSIDERATION

On June 16, 1999, the Subcommittee on Telecommunications, Trade, and Consumer Protection met in open markup session and approved H.R. 850, the Security And Freedom through Encryption (SAFE) Act, for Full Committee consideration, amended, by a voice vote. On June 23, 1999, the Full Committee met in open markup session and ordered H.R. 850 reported to the House, amended, by a voice vote, a quorum being present.

COMMITTEE VOTES

Clause 3(b) of rule XIII of the Rules of the House requires the Committee to list the record votes on the motion to report legislation and amendments thereto. There were no record votes taken in connection with ordering H.R. 850, the Security And Freedom through Encryption (SAFE) Act, reported. The following amendments were considered and agreed to by voice votes:

An Amendment by Mr. Oxley, No. 1, to clarify that because a product may be allowed to be exported under this bill because it has encryption capabilities does not prevent the Secretary of Commerce from prohibiting its export for other reasons;

An Amendment by Mr. Dingell, No. 2, to require that in order for a U.S. manufacturer to export a product to a particular country a comparable security product must be commercially available in that particular country;

An Amendment by Mr. Oxley, No. 3, to expand the list of reasons for which the Secretary of Commerce can deny the export of encryption products to specific groups and organizations to include: (A) used to harm national security, (B) used to sexually exploit children, or (C) used for illegal activities by organized crime;

An Amendment by Mr. Oxley, No. 4, to require the Secretary of Commerce to consult with the Secretary of Defense, the Secretary of State, the Attorney General, and the Director of the Central Intelligence Agency when conducting a technical review of an encryption product for export;

An Amendment by Mr. Stearns, No. 6, to prohibit the ability of U.S. companies to export products to the People's Liberation Army or Communist Chinese Military; and

An Amendment by Mr. Stearns, No. 7, to require that if a person was served a subpoena for access to encrypted information and if the person had the capability to decrypt the information but did not, then the person would be subject to additional criminal penalties.

In addition, the following amendments were offered and withdrawn by unanimous consent:

An Amendment by Mr. Oxley, No. 5, to allow Federal government agencies to condition their contracts with the private sector to require use of a particular encryption technology (e.g., recoverable encryption products); and

A unanimous consent request by Mr. Tauzin to amend the Oxley Amendment by adding "to assist in the performance of national security or law enforcement function" in line 4, after the word "entity".

A second unanimous consent request by Mr. Tauzin to amend the Oxley Amendment by striking "with a non-Government entity" in line 4 and inserting in lieu thereof "performing national security or law enforcement functions with a non-Government entity", was pending when the Oxley Amendment was withdrawn by unanimous consent.

A motion by Mr. Bliley to order H.R. 850 reported to the House, amended, was agreed to by a voice vote, a quorum being present.

COMMITTEE OVERSIGHT FINDINGS

Pursuant to clause 3(c)(1) of rule XIII of the Rules of the House of Representatives, the Committee held a legislative hearing and made findings that are reflected in this report.

COMMITTEE ON GOVERNMENT REFORM OVERSIGHT FINDINGS

Pursuant to clause 3(c)(4) of rule XIII of the Rules of the House of Representatives, no oversight findings have been submitted to the Committee by the Committee on Government Reform.

NEW BUDGET AUTHORITY, ENTITLEMENT AUTHORITY, AND TAX EXPENDITURES

In compliance with clause 3(c)(2) of rule XIII of the Rules of the House of Representatives, the Committee finds that H.R. 850, the Security And Freedom through Encryption (SAFE) Act, would result in no new or increased budget authority, entitlement authority, or tax expenditures or revenues.

COMMITTEE COST ESTIMATE

The Committee adopts as its own the cost estimate prepared by the Director of the Congressional Budget Office pursuant to section 402 of the Congressional Budget Act of 1974.

CONGRESSIONAL BUDGET OFFICE ESTIMATE

Pursuant to clause 3(c)(3) of rule XIII of the Rules of the House of Representatives, the following is the cost estimate provided by the Congressional Budget Office pursuant to section 402 of the Congressional Budget Act of 1974:

U.S. CONGRESS,
CONGRESSIONAL BUDGET OFFICE,
Washington, DC, July 1, 1999.

Hon. TOM BLILEY,
Chairman, Committee on Commerce,
House of Representatives, Washington, DC.

DEAR MR. CHAIRMAN: The Congressional Budget Office has prepared the enclosed cost estimate for H.R. 850, 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 Mark Hadley and Mark Grabowicz (for federal costs), and Shelley Finlayson (for the state and local impact).

Sincerely,

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

Enclosure.

H.R. 850—Security and Freedom Through Encryption (SAFE) Act

Summary: H.R. 850 would allow individuals in the United States to use and sell any form of encryption and would prohibit states or the federal government from requiring individuals to relinquish the key to encryption products. The bill also would prevent the Department of Commerce (DOC) from restricting the export of most nonmilitary encryption products. H.R. 850 would establish a National Electronic Technologies (NET) Center within DOC's National Telecommunications and Information Administration (NTIA) to provide assistance and information on encryption products to law enforcement officials. The bill also would require the Attorney General to maintain data on the instances in which encryption impedes or obstructs the ability of the Department of Justice (DOJ) to enforce criminal laws. Finally, the bill would establish criminal penalties and fines for the use of encryption technologies to conceal incriminating information related to a felony, for transferring certain encryption products to the military of the People's Republic of China, and for providing information that is required by a court order in only an encrypted format.

Assuming the appropriation of the necessary amounts, CBO estimates that enacting this bill would result in additional discretionary spending by DOC and DOJ of at least $25 million over the 2000–2004 period. Enacting H.R. 850 also would affect direct spending and receipts. Therefore, pay-as-you-go procedures would apply. CBO estimates, however, that the amounts of additional direct spending and receipts would not be significant.

H.R. 850 contains intergovernmental mandates on state governments as defined in the Unfunded Mandates Reform Act (UMRA). CBO estimates that states would not incur any costs to comply

with the mandates, and that local and tribal governments would not be affected by the bill. H.R. 850 contains no new private-sector mandates as defined in UMRA.

Estimated cost to the Federal Government: CBO estimates that implementing H.R. 850 would increase discretionary costs for DOC and DOJ by about $5 million a year over the 2000–2004 period. The costs of this legislation fall within budget function 370 (commerce and housing credit) and 750 (administration of justice). Direct spending and revenues would also increase, but by less than $500,000 a year.

Spending subject to appropriation

Under current policy, BXA would likely spend about $500,000 a year reviewing exports of encryption products, assuming appropriation of the necessary amounts. In November 1996, the Administration issued an executive order and memorandum that authorized BXA to control the export of all nonmilitary encryption products. If H.R. 850 were enacted, BXA would still be required to review requests to export most computer hardware with encryption capabilities but would not be required to review most requests to export computer software with encryption capabilities. Within two years of enactment, H.R. 850 would shift such responsibilities and the associated costs from BXA to NTIA. Thus, CBO estimates that implementing H.R. 850 not significantly change costs to DOC to control exports of nonmilitary encryption products.

H.R. 850 would require the Secretary of Commerce to conduct a number of studies on electronic commerce and domestic and foreign impediments to trade in encryption products. Based on information from the Department of Commerce, CBO estimates that completing the required studies would cost about $1 million in fiscal year 2000, assuming appropriation of the necessary funds.

H.R. 850 would establish within NTIA the NET Center, which would assist federal, state, and local law enforcement agencies with issues involving encryption and information security. The bill would assign the NET Center a broad range of duties, including providing information and assistance, serving as an information clearinghouse, and conducting research. The costs to establish and operate the NET Center would depend on the extent to which service would be provided to the law enforcement community nationwide. Based on information from DOC, we estimate that the minimum costs to fulfill the bill's requirements would be roughly $4 million annually, but the costs could be much greater. Any spending relating to the NET Center would be subject to the availability of appropriations.

DOJ would also be required to collect and maintain data on the instances in which encryption impedes or obstructs the ability of the agency to enforce criminal laws. CBO projects that collecting and maintaining the data would cost DOJ between $500,000 and $1 million a year. Because H.R. 850 would establish new federal crimes, CBO anticipates that the U.S. government would be able to pursue cases that it otherwise would be unable to prosecute. Based on information from DOJ, however, we do not expect the government to pursue many additional cases. Thus, CBO estimates

that implementing these provisions would not have a significant impact on the cost of federal law enforcement activity.

Direct spending and revenues

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

Direct spending and revenues also could result from the provision that would allow the NET Center to accept donations to further its work. CBO expects that the amount of any contributions (recorded in the budget as revenues) would be less than $500,000 a year, and that they would be used in the same year as they were received. Therefore, we estimate that the net budgetary impact of the gift authority granted to the NET Center would be negligible for all years.

Pay-as-you-go considerations: The Balanced Budget and Emergency Control Act sets up pay-as-you-go procedures for legislation affecting direct spending or receipts. H.R. 850 would affect direct spending and receipts by imposing criminal fines and by allowing the new NET Center to accept donations. CBO estimates that the amounts of additional direct spending and receipts would not be significant.

Estimated impact on State, local, and tribal governments: H.R. 850 would preempt state law by prohibiting states from setting standards for encryption products or methodology. The bill would also prohibit states from requiring persons to build decryption keys into computer hardware or software, make decryption keys available to another person or entity, or retain encryption keys. These preemptions would be mandates as defined by UMRA. However, states would bear no costs as the result of the mandates because none currently require the availability of such keys or require private individuals to use a particular encryption standard.

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

Previous CBO estimates: On April 21, 1999, CBO transmitted a cost estimate for H.R. 850 as ordered reported by the House Committee on the Judiciary on May 24, 1999. CBO estimated that the Judiciary Committee's version would increase total discretionary costs over the 2000–2004 period by between $3 million and $5 million. In comparison, CBO estimates that implementing this version of the bill would cost at least $25 million over the same period.

Estimate prepared by: Federal Costs: Mark Hadley and Mark Grabowicz. Impact on State, Local and Tribal Governments: Shelly Finlayson.

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

FEDERAL MANDATES STATEMENT

The Committee adopts as its own the estimate of Federal mandates prepared by the Director of the Congressional Budget Office pursuant to section 423 of the Unfunded Mandates Reform Act.

ADVISORY COMMITTEE STATEMENT

Section 9 of H.R. 850 creates an Advisory Board of the Strategic NET Center to advise the Federal government on new technologies relating to encryption. Pursuant to the requirements of subsection 5(b) of the Federal Advisory Committee Act, the Committee finds that the functions of the proposed advisory committee are not and cannot be performed by an existing Federal agency or advisory commission or by enlarging the mandate of an existing advisory committee.

CONSTITUTIONAL AUTHORITY STATEMENT

Pursuant to clause 3(d)(1) of rule XIII of the Rules of the House of Representatives, the Committee finds that the Constitutional authority for this legislation is provided in Article I, section 8, clause 3, which grants Congress the power to regulate commerce with foreign nations, among the several States, and with the Indian tribes.

APPLICABILITY TO LEGISLATIVE BRANCH

The Committee finds that the legislation does not relate to the terms and conditions of employment or access to public services or accommodations within the meaning of section 102(b)(3) of the Congressional Accountability Act.

SECTION-BY-SECTION ANALYSIS OF THE LEGISLATION

Section 1. Short title

Section 1 establishes the short title of the bill as the "Security And Freedom through Encryption (SAFE) Act."

Section 2. Definitions

Section 2 provides for definitions of terms to be used in the bill including "computer hardware," "encrypt or encryption," "encryption product," "key," "key recovery information," "person," "Secretary," "State," and "United States person." In addition, section 2 ties the definitions of "wire communications" and "electronic communications" to their definitions contained in the existing Federal wiretap statute, section 2510 et seq. of title 18, U.S. Code.

Section 3. Ensuring development and deployment of encryption is a voluntary private sector activity

Section 3(a) establishes as policy that the use, development, manufacture, sale, distribution, and importation of encryption products used for confidentiality, authenticity, or integrity be voluntary and market driven. Section 3(b) prohibits the Federal government or any State from conditioning, tying, or linking the encryption products, standards, or services used for confidentiality with those used for authentication or integrity purposes.

Section 4. Protection of domestic sale and use of encryption

Section 4 codifies current policy that it is lawful for a person within any State or any United States person in a foreign country to use any encryption product, regardless of the encryption algorithm selected, encryption length chosen, existence of key recovery, other plaintext access capability, or implementation or medium used.

Section 5. Prohibition on mandatory government access to plaintext

Section 5(a) prohibits the Federal government or a State from requiring, conditioning approval, providing incentives for, or tying any benefit to a requirement that a decryption key, access to a key, key recovery information, or any other plaintext access capability be: (1) built into any hardware or software; (2) given to any person; or (3) retained by the owner or user of an encryption key or any other person.

Section 5(b) provides an exception to subsection (a) for access by law enforcement officers or any member of the intelligence community acting pursuant to lawful authority to require a party to provide access to encrypted communications or information.

Section 6. Unlawful use of encryption in furtherance of a criminal act

Section 6(a) makes it a crime to knowingly and willfully encrypt incriminating communications or information relating to a felony with the intent to conceal information in order to avoid detection by law enforcement agencies or prosecution. A person found guilty of this offense may be fined, imprisoned for not more than 5 years, or both. Second and subsequent offenses may result in a fine, imprisonment of not more than 10 years, or both.

Section 6(b) states that the use of encryption cannot, by itself, be the basis for establishing probable cause with respect to a criminal offense or a search warrant.

Section 7. Exports of encryption

Section 7(a) of the bill would amend the Export Administration Act of 1979 to add a new section 17(g).

New subsection (g)(1) provides the Secretary of Commerce (the Secretary) with exclusive authority over the export control of all encryption related products and equipment, except those designed or modified for military use. New subsection (g)(2) requires the Administrator of the National Telecommunications and Information Administration (NTIA) to identify, define, and determine which encryption products are designed for improvement of network security, network reliability, or data security. New subsection (g)(2) also requires the Secretary to delegate, within a two year period from the date of enactment, authority for all export determinations and technical product reviews for encryption products used to improve network reliability, network security and data security to NTIA within the Department of Commerce. The Secretary is given authority to further delegate other encryption products beyond those identified in subparagraph (A) to NTIA.

New subsection (g)(3) requires the Secretary, after a 30 working day technical review (which includes consultation with the Depart-

ments of Defense, State, and Justice, and the Central Intelligence Agency) of each encryption product, to provide for the export of encryption products without a license for generally available encryption software and hardware products, generally available products containing encryption, generally available products with encryption capabilities, technical assistance and data used to install or maintain generally available encryption products, products containing encryption, products with encryption capabilities, and encryption products not used for confidentiality purposes.

New subsection (g)(4) requires the Secretary, after a 30 working day technical review (which includes consultation with the Departments of Defense, State, and Justice, and the Central Intelligence Agency) of each encryption product, to allow the export of custom-designed encryption products and custom-designed products with encryption capabilities if those products are permitted for use by international financial institutions or if comparable products are commercially available in such country. An exception to this subsection exists if there is substantial evidence that these products will be used: (1) for military or terrorist end-use, or modified for military or terrorist end-use; (2) to harm U.S. national security, including U.S. capabilities fighting drug trafficking, terrorism, or espionage; (3) in illegal activities involving sexual exploitation of, abuse of, or sexually explicit conduct with minors; or (4) in illegal activities involving organized crime. New subsection (g)(5) provides definitions for "computer hardware," "computing device," "customer premises equipment," "data security," "encryption," "generally available," "network reliability," "network security," "technical assistance," "technical data," and "technical review."

Section 7(b) amends section 103(b) of the National Telecommunications and Information Administration Organization Act to provide specific authority to carry out the functions relating to export determinations and technical product reviews of encryption products used for network security, network reliability, or data security, as added by section 7(a). Section 7(c) prevents the Secretary from requiring export licenses for products that as of the date of enactment of the bill are not required to have one.

Section 7(d)(1) provides a savings clause to make clear that nothing in the bill affects the President's authority under the International Emergency Economic Powers Act, the Trading with the Enemy Act, or the Export Administration Act of 1979 to prohibit the export of encryption products to terrorist nations or nations that have been determined to repeatedly support acts of international terrorism, or to impose an embargo on exports to and imports from a specific country. Section 7(d)(2) provides the Secretary of Commerce authority to prohibit the export to an individual or organization in a specified foreign country of a specific encryption product if there is substantial evidence that the product will be used: (1) for military or terrorist end-use, or modified for military or terrorist end-use; (2) to harm U.S. national security, including U.S. capabilities fighting drug trafficking, terrorism, or espionage; (3) in illegal activities involving sexual exploitation of, abuse of, or sexually explicit conduct with minors; or (4) in illegal activities involving organized crime. Section 7(d)(3) provides a savings clause to make clear that nothing in the bill prevents the Secretary from

denying the export of products with encryption capabilities for other reasons than encryption.

Section 7(e) deems that the Export Administration Act of 1979 be in effect for the purpose of carrying out the amendment contained in this section of the bill.

Section 8. Government procurement of encryption products

Section 8 clarifies Federal procurement policy with regard to encryption products. Section 8(a) establishes that it is the policy of the United States to promote public interaction with the government while promoting privacy and security for electronic communications or stored information.

Section 8(b) clarifies that a Federal government agency, department or instrumentality is permitted without restriction to purchase and use encryption products of any nature for their own internal purposes. Conversely, section 8(c) prevents the Federal government from using its transactions with the private sector through contracts, procurement, individual contacts and the like to be a mechanism to encourage or mandate the use of any type of encryption product.

Section 9. National Electronic Technologies Center

Section 9 amends Part A of the National Telecommunications and Information Administration Organization Act to add a new section 106.

New section 106 establishes within NTIA a National Electronic Technologies Center (referred to as the "NET Center"). The primary purpose of the NET Center is to provide technical assistance to law enforcement agencies so that they may cope with new technology challenges. Specifically, the NET Center will be responsible for serving as a national center for Federal, State, and local law enforcement authorities for information and assistance regarding decryption. It will also serve as a national center where industry and government can gather to exchange information regarding data security. In addition, the NET Center will be required to: (1) examine encryption techniques and methods to facilitate the ability of law enforcement to gain access to plaintext of communications and electronic information; (2) conduct research to improve law enforcement's means of access to encrypted communications; (3) determine whether other techniques can be used to help law enforcement access communications and electronic information; and (4) obtain information regarding the most current computer hardware, computer software, and telecommunications equipment to understand how best to access communications.

Administratively, the Administrator of NTIA will appoint the Director of the NET Center and the Director will be responsible for hiring personnel that he or she determines is necessary to carry out the duties of the NET Center. Other Federal government agencies may also "loan" personnel to the NET Center or provide facilities, information, and other non-personnel resources. In addition, the NET Center may accept donations in the form of money, services, or property from the private sector to help it function. Such donations shall be deposited in the Treasury and shall be available for disbursement upon order of the Director.

Within two months after the date of enactment of this Act, the Administrator of NTIA will be required to develop a plan for the establishment of the NET Center. The plan must be published in the Federal Register and must identify: the physical location of the NET Center; equipment, software, and personnel necessary for the NET Center to function; the amount of funding necessary to establish and operate the NET Center; and sources of probable funding for the NET Center, including any sources of in-kind contributions from private industry.

In addition, new section 106(h) creates an Advisory Board of the NET Center, which is intended to advise the government on new technologies relating to encryption. The Administrator of NTIA is required to appoint a chairman of the Advisory Board and members of the Advisory Board must have technical expertise in the field of encryption, decryption, electronic communication, information security, electronic commerce, or law enforcement. More specifically, the purpose of the Advisory Board is to advise the NET Center and the Federal government regarding new and emerging technologies relating to encryption and decryption of communications and electronic information.

Section 10. Study of network and data security issues

Section 10 amends Part C of the National Telecommunications and Information Administration Organization Act to add a new section 156.

New section 156(a) requires NTIA to conduct an annual in-depth analysis of: (1) the relationship between network reliability, network security, and data security and the conduct of transactions in interstate commerce; (2) the availability of various methods for encrypting communications; and, (3) the effects of various methods on providing access to encrypted communications and to information to further law enforcement activities.

New section 156(b) requires NTIA to specifically examine on the current availability and availability expected in one year of the encryption products that meet or would meet the tests under section 7 of the bill, as reported by the Committee on Commerce, and thus qualify to be exported. While section 7 provides extensive definitions to help clarify what encryption products would qualify for export relief, there will still be some debate and dispute over certain encryption products. New subsection (b) is intended to provide an examination of the products as they exist in the marketplace and those products that are expected to be available within a one year time period. The forward-looking aspect of this provision will provide industry and government a very good vision of what is expected to come to market in the near future.

New subsection 156(c) requires NTIA to report to Congress and the President within one year, and annually thereafter, on its findings under this section. New section 156(d) states that definitions of "data security," "encryption," "network reliability," and "network security" have the same meaning as contained in the Export Administration Act of 1979, as amended by this bill, and that the definitions of "Internet" and "interactive computer systems" have the same meaning as contained in the Communications Act of 1934.

Section 11. Treatment of encryption in interstate and foreign commerce

Section 11 requires the Secretary of Commerce to undertake certain activities in order to promote the export of U.S. encryption products in the global market. Through such instruction to the Secretary of Commerce, the Committee intends to promote robust participation by U.S. firms in the development of global electronic commerce. The Committee is concerned that as U.S. export policy with regards to encryption products is relaxed, through passage of this legislation, other countries may attempt to impose import barriers as a mechanism to maintain the status quo with regards to the availability of U.S. encryption products. Section 11 is intended to address this real possibility by requiring active, positive action by the Administration in order to prevent this from happening.

Subsection (a) requires the Secretary of Commerce to complete an inquiry within 180 days of the enactment of this Act to identify both domestic and foreign impediments to trade in encryption products and services. Such an inquiry would include the identification of import restrictions maintained by other countries that constitute unfair barriers. The inquiry would also include an examination of U.S. regulations, such as export restrictions, that may actually impede trade in encryption products and services.

Subsection (b) requires the Secretary to adopt regulations within one year of the Act's enactment that are intended to reduce foreign and domestic impediments to encryption products and services. The regulations must be designed to promote the sale in foreign markets of U.S. encryption products and services, including through strengthening the competitiveness of U.S. providers of such products and services.

Subsection (c)(1) requires that upon completion of the six-month inquiry into foreign and domestic impediments to trade in encryption products and services, the Secretary of Commerce shall submit a report to the President on his or her findings. The report must include a determination by the Secretary on what impediments may require international negotiation to reduce.

Subsection (c)(2) requires the President to negotiate with other countries for agreements designed to promote encryption products and services and to achieve mutual recognition of export controls. Export controls may be designed to preserve countries' national security, safeguard privacy interests, and prevent commercial espionage. Mutual recognition of export controls will promote the sale in foreign commerce of U.S. encryption products and services by facilitating a common approach by the U.S. and our trading partners. Subsection (c)(2) also enables the President to consider a country's refusal to negotiate such agreements when considering U.S. participation in an assistance or cooperation program with that country. Finally, the subsection requires the President to submit a report to the Congress regarding the status of international efforts on encryption not later than December 31, 2000.

Section 12. Collection of information on effect of encryption on law enforcement activities

Section 12(a) requires the Attorney General to compile information on instances in which encryption has interfered with, impeded,

or obstructed the ability of the Department of Justice to enforce Federal criminal law and to maintain that information in classified form. Subsection (b) requires that the Attorney General shall make the information compiled under subsection (a), including an unclassified summary, available to Members of Congress upon request.

Section 13. Prohibition on transfers to PLA and Communist Chinese military companies

Section 13 adds new criminal penalties for knowingly and willfully exporting encryption products above 56 bits to the People's Liberation Army or to any Communist Chinese military company. Under section 13(a), a person found guilty of this offense may be fined, imprisoned for not more than 5 years, or both. Second and subsequent offenses may result in a fine, imprisonment of not more than 10 years, or both.

Section 13(b) provides definitions used in the section, including "Communist Chinese military company." The Committee notes that this definition will be based on section 1237(b)(2) of the Strom Thurmond National Defense Authorization Act for Fiscal Year 1999 once the Administration complies with the requirement to identify and list such companies.

Section 14. Failure to decrypt information obtained under court order

Section 14 adds new criminal penalties for individuals that fail to comply with a court order to provide access to encrypted information if they have possession of the key or other such capabilities to decrypt the information into a readable or comprehensive manner prior to its encryption. Under section 14, a person found guilty of this offense may be fined, imprisoned for not more than 5 years, or both. Second and subsequent offenses may result in a fine, imprisonment of not more than 10 years, or both. The Committee does not expect that the interpretation of "such capabilities" will be expanded to interfere with an individual's right not to self-incriminate himself or herself under protection afforded by the Fifth Amendment to the U.S. Constitution.

CHANGES IN EXISTING LAW MADE BY THE BILL, AS REPORTED

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

SECTION 17 OF THE EXPORT ADMINISTRATION ACT OF 1979

EFFECT ON OTHER ACTS

SEC. 17. (a) * * *

* * * * * * *

(g) CERTAIN CONSUMER PRODUCTS, COMPUTERS, AND RELATED EQUIPMENT.—

(1) GENERAL RULE.—Subject to paragraphs (2), (3), and (4), the Secretary shall have exclusive authority to control exports of all computer hardware, software, computing devices, customer premises equipment, communications network equipment, and technology for information security (including encryption), except that which is specifically designed or modified for military use, including command, control, and intelligence applications.

(2) CRITICAL INFRASTRUCTURE PROTECTION PRODUCTS.—

(A) IDENTIFICATION.—Not later than 90 days after the date of the enactment of the Security And Freedom through Encryption (SAFE) Act, the Assistant Secretary of Commerce for Communications and Information and the National Telecommunications and Information Administration shall issue regulations that identify, define, or determine which products and equipment described in paragraph (1) are designed for improvement of network security, network reliability, or data security.

(B) NTIA RESPONSIBILITY.—Not later than the expiration of the 2-year period beginning on the date of the enactment of the Security And Freedom through Encryption (SAFE) Act, all authority of the Secretary under this subsection and all determinations and reviews required by this section, with respect to products and equipment described in paragraph (1) that are designed for improvement of network security, network reliability, or data security through the use of encryption, shall be exercised through and made by the Assistant Secretary of Commerce for Communications and Information and the National Telecommunications and Information Administration. The Secretary may, at any time, assign to the Assistant Secretary and the NTIA authority of the Secretary under this section with respect to other products and equipment described in paragraph (1).

(3) ITEMS NOT REQUIRING LICENSES.—After a one-time technical review by the Secretary of not more than 30 working days, which shall include consultation with the Secretary of Defense, the Secretary of State, the Attorney General, and the Director of Central Intelligence, no export license may be required, except pursuant to the Trading with the Enemy Act or the International Emergency Economic Powers Act (but only to the extent that the authority of such Act is not exercised to extend controls imposed under this Act), for the export or reexport of—

(A) any computer hardware or software or computing device, including computer hardware or software or computing devices with encryption capabilities—

(i) that is generally available;

(ii) that is in the public domain for which copyright or other protection is not available under title 17, United States Code, or that is available to the public because it is generally accessible to the interested public in any form; or

(iii) that is used in a commercial, off-the-shelf, consumer product or any component or subassembly de-

signed for use in such a consumer product available within the United States or abroad which—

(I) includes encryption capabilities which are inaccessible to the end user; and

(II) is not designed for military or intelligence end use;

(B) any computing device solely because it incorporates or employs in any form—

(i) computer hardware or software (including computer hardware or software with encryption capabilities) that is exempted from any requirement for a license under subparagraph (A); or

(ii) computer hardware or software that is no more technically complex in its encryption capabilities than computer hardware or software that is exempted from any requirement for a license under subparagraph (A) but is not designed for installation by the purchaser;

(C) any computer hardware or software or computing device solely on the basis that it incorporates or employs in any form interface mechanisms for interaction with other computer hardware or software or computing devices, including computer hardware and software and computing devices with encryption capabilities;

(D) any computing or telecommunication device which incorporates or employs in any form computer hardware or software encryption capabilities which—

(i) are not directly available to the end user; or

(ii) limit the encryption to be point-to-point from the user to a central communications point or link and does not enable end-to-end user encryption;

(E) technical assistance and technical data used for the installation or maintenance of computer hardware or software or computing devices with encryption capabilities covered under this subsection; or

(F) any encryption hardware or software or computing device not used for confidentiality purposes, such as authentication, integrity, electronic signatures, nonrepudiation, or copy protection.

(4) COMPUTER HARDWARE OR SOFTWARE OR COMPUTING DEVICES WITH ENCRYPTION CAPABILITIES.—After a one-time technical review by the Secretary of not more than 30 working days, which shall include consultation with the Secretary of Defense, the Secretary of State, the Attorney General, and the Director of Central Intelligence, the Secretary shall authorize the export or reexport of computer hardware or software or computing devices with encryption capabilities for nonmilitary end uses in any country—

(A) to which exports of computer hardware or software or computing devices of comparable strength are permitted for use by financial institutions not controlled in fact by United States persons, unless there is substantial evidence that such computer hardware or software or computing devices will be—

(i) diverted to a military end use or an end use supporting international terrorism;

(ii) modified for military or terrorist end use;

(iii) reexported without any authorization by the United States that may be required under this Act; or

(iv)(I) harmful to the national security of the United States, including capabilities of the United States in fighting drug trafficking, terrorism, or espionage, (II) used in illegal activities involving the sexual exploitation of, abuse of, or sexually explicit conduct with minors (including activities in violation of chapter 110 of title 18, United States Code, and section 2423 of such title), or (III) used in illegal activities involving organized crime; or

(B) if the Secretary determines that a computer hardware or software or computing device offering comparable security is commercially available in such country from a foreign supplier, without effective restrictions.

(5) DEFINITIONS.—For purposes of this subsection—

(A) the term "computer hardware" has the meaning given such term in section 2 of the Security And Freedom through Encryption (SAFE) Act;

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

(C) the term "customer premises equipment" means equipment employed on the premises of a person to originate, route, or terminate communications;

(D) the term "data security" means the protection, through techniques used by individual computer and communications users, of data from unauthorized penetration, manipulation, or disclosure;

(E) the term "encryption" has the meaning given such term in section 2 of the Security And Freedom through Encryption (SAFE) Act;

(F) the term "generally available" means, in the case of computer hardware or computer software (including computer hardware or computer software with encryption capabilities)—

(i) computer hardware or computer software that is—

(I) distributed through the Internet;

(II) offered for sale, license, or transfer to any person without restriction, whether or not for consideration, including, but not limited to, over-the-counter retail sales, mail order transactions, phone order transactions, electronic distribution, or sale on approval;

(III) preloaded on computer hardware or computing devices that are widely available for sale to the public; or

(IV) assembled from computer hardware or computer software components that are widely available for sale to the public;

(ii) not designed, developed, or tailored by the manufacturer for specific purchasers or users, except that any such purchaser or user may—

(I) supply certain installation parameters needed by the computer hardware or software to function properly with the computer system of the user or purchaser; or

(II) select from among options contained in the computer hardware or computer software; and

(iii) with respect to which the manufacturer of that computer hardware or computer software—

(I) intended for the user or purchaser, including any licensee or transferee, to install the computer hardware or software and has supplied the necessary instructions to do so, except that the manufacturer of the computer hardware or software, or any agent of such manufacturer, may also provide telephone or electronic mail help line services for installation, electronic transmission, or basic operations; and

(II) the computer hardware or software is designed for such installation by the user or purchaser without further substantial support by the manufacturer;

(G) the term "network reliability" means the prevention, through techniques used by providers of computer and communications services, of the malfunction, and the promotion of the continued operations, of computer or communications network;

(H) the term "network security" means the prevention, through techniques used by providers of computer and communications services, of unauthorized penetration, manipulation, or disclosure of information of a computer or communications network;

(I) the term "technical assistance" includes instruction, skills training, working knowledge, consulting services, and the transfer of technical data;

(J) the term "technical data" includes blueprints, plans, diagrams, models, formulas, tables, engineering designs and specifications, and manuals and instructions written or recorded on other media or devices such as disks, tapes, or read-only memories; and

(K) the term "technical review" means a review by the Secretary of computer hardware or software or computing devices with encryption capabilities, based on information about the product's encryption capabilities supplied by the manufacturer, that the computer hardware or software or computing device works as represented.

NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION ORGANIZATION ACT

* * * * * * *

TITLE I—NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION

PART A—ORGANIZATION AND FUNCTIONS

* * * * * * *

SEC. 103. ESTABLISHMENT; ASSIGNED FUNCTIONS.

(a) * * *

(b) ASSIGNED FUNCTIONS.—

(1) * * *

* * * * * * *

(4) EXPORT OF COMMUNICATIONS TRANSACTION TECHNOLOGIES.—In accordance with section 17(g)(2) of the Export Administration Act of 1979 (50 U.S.C. App. 2416(g)(2)), the Secretary shall assign to the Assistant Secretary and the NTIA the authority of the Secretary under such section 17(g), with respect to products and equipment described in paragraph (1) of such section that are designed for improvement of network security, network reliability, or data security, that (after the expiration of the 2-year period beginning on the date of the enactment of the Security And Freedom through Encryption (SAFE) Act) is to be exercised by the Assistant Secretary and the NTIA.

* * * * * * *

SEC. 106. NATIONAL ELECTRONIC TECHNOLOGIES CENTER.

(a) ESTABLISHMENT.—There is established in the NTIA a National Electronic Technologies Center (in this section referred to as the "NET Center").

(b) DIRECTOR.—The NET Center shall have a Director, who shall be appointed by the Assistant Secretary.

(c) DUTIES.—The duties of the NET Center shall be—

(1) to serve as a center for industry and government entities to exchange information and methodology regarding data security techniques and technologies;

(2) to examine encryption techniques and methods to facilitate the ability of law enforcement to gain efficient access to plaintext of communications and electronic information;

(3) to conduct research to develop efficient methods, and improve the efficiency of existing methods, of accessing plaintext of communications and electronic information;

(4) to investigate and research new and emerging techniques and technologies to facilitate access to communications and electronic information, including —

(A) reverse-steganography;

(B) decompression of information that previously has been compressed for transmission; and

(C) de-multiplexing;

(5) to obtain information regarding the most current computer hardware and software, telecommunications, and other capabilities to understand how to access information transmitted across computer and communications networks; and

(6) to serve as a center for Federal, State, and local law enforcement authorities for information and assistance regarding decryption and other access requirements.

(d) EQUAL ACCESS.—State and local law enforcement agencies and authorities shall have access to information, services, resources, and assistance provided by the NET Center to the same extent that Federal law enforcement agencies and authorities have such access.

(e) PERSONNEL.—The Director may appoint such personnel as the Director considers appropriate to carry out the duties of the NET Center.

(f) ASSISTANCE OF OTHER FEDERAL AGENCIES.—Upon the request of the Director of the NET Center, the head of any department or agency of the Federal Government may, to assist the NET Center in carrying out its duties under this section—

(1) detail, on a reimbursable basis, any of the personnel of such department or agency to the NET Center; and

(2) provide to the NET Center facilities, information, and other non-personnel resources.

(g) PRIVATE INDUSTRY ASSISTANCE.—The NET Center may accept, use, and dispose of gifts, bequests, or devises of money, services, or property, both real and personal, for the purpose of aiding or facilitating the work of the Center. Gifts, bequests, or devises of money and proceeds from sales of other property received as gifts, bequests, or devises shall be deposited in the Treasury and shall be available for disbursement upon order of the Director of the NET Center.

(h) ADVISORY BOARD.—

(1) ESTABLISHMENT.—There is established the Advisory Board of the NET Center (in this subsection referred to as the "Advisory Board"), which shall be comprised of 11 members who shall have the qualifications described in paragraph (2) and who shall be appointed by the Assistant Secretary not later than 6 months after the date of the enactment of this Act. The chairman of the Advisory Board shall be designated by the Assistant Secretary at the time of appointment.

(2) QUALIFICATIONS.—Each member of the Advisory Board shall have experience or expertise in the field of encryption, decryption, electronic communication, information security, electronic commerce, or law enforcement.

(3) DUTIES.—The duty of the Advisory Board shall be to advise the NET Center and the Federal Government regarding new and emerging technologies relating to encryption and decryption of communications and electronic information.

(i) IMPLEMENTATION PLAN.—Within 2 months after the date of the enactment of this Act, the Assistant Secretary, in consultation and cooperation with other appropriate Federal agencies and appropriate industry participants, develop and cause to be published in the Federal Register a plan for establishing the NET Center. The plan shall—

(1) specify the physical location of the NET Center and the equipment, software, and personnel resources necessary to carry out the duties of the NET Center under this section;

(2) assess the amount of funding necessary to establish and operate the NET Center; and

(3) identify sources of probable funding for the NET Center, including any sources of in-kind contributions from private industry.

* * * * * * *

PART C—SPECIAL AND TEMPORARY PROVISIONS

* * * * * * *

SEC. 156. STUDY OF NETWORK RELIABILITY AND SECURITY AND DATA SECURITY ISSUES.

(a) IN GENERAL.—The NTIA shall conduct an examination of—

(1) the relationship between—

(A) network reliability (for communications and computer networks), network security (for such networks), and data security issues; and

(B) the conduct, in interstate commerce, of electronic commerce transactions, including through the medium of the telecommunications networks, the Internet, or other interactive computer systems;

(2) the availability of various methods for encrypting communications; and

(3) the effects of various methods of providing access to encrypted communications and to information to further law enforcement activities.

(b) SPECIFIC ISSUES.—In conducting the examination required by subsection (a), the NTIA shall—

(1) analyze and evaluate the requirements under paragraphs (3) and (4) of section 17(g) of the Export Administration Act of 1979 (50 U.S.C. App. 2416(g); as added by section 7(a) of this Act) for products referred to in such paragraphs to qualify for the license exemption or mandatory export authorization under such paragraphs, and determine—

(A) the scope and applicability of such requirements and the products that, at the time of the examination, qualify for such license exemption or export authorization; and

(B) the products that will, 12 months after the examination is conducted, qualify for such license exemption or export authorization; and

(2) assess possible methods for providing access to encrypted communications and to information to further law enforcement activities.

(c) REPORTS.—Within one year after the date of enactment of this section, the NTIA shall submit to the Congress and the President a detailed report on the examination required by subsections (a) and (b). Annually thereafter, the NTIA shall submit to the Congress and the President an update on such report.

(d) DEFINITIONS.—For purposes of this section—

(1) the terms "data security", "encryption", "network reliability", and "network security" have the meanings given such terms in section 17(g)(5) of the Export Administration Act of 1979 (50 U.S.C. App. 2416(g)(5)); and

(2) the terms "Internet" and "interactive computer systems" have the meanings provided by section 230(e) of the Communications Act of 1934 (47 U.S.C. 230(e)).

* * * * * * *

○