105TH CONGRESS } HOUSE OF REPRESENTATIVES { REPT. 105–108
1st Session } { Part 5

SECURITY AND FREEDOM THROUGH ENCRYPTION (SAFE) ACT

SEPTEMBER 29, 1997.—Committed to the Committee of the Whole House on the State of the Union and ordered to be printed

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

REPORT

together with

DISSENTING AND ADDITIONAL VIEWS

[To accompany H.R. 695]

[Including cost estimate of the Congressional Budget Office]

The Committee on Commerce, to whom was referred the bill (H.R. 695) to amend title 18, United States Code, to affirm the rights of United States persons to use and sell encryption and to relax export controls on encryption, having considered the same, report favorably thereon with an amendment and recommend that the bill as amended do pass.

CONTENTS

43–673

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. SALE AND USE OF ENCRYPTION.

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

"CHAPTER 125—ENCRYPTED WIRE AND ELECTRONIC INFORMATION

"§ 2801. Definitions

"As used in this chapter—

"(1) the terms 'person', 'State', 'wire communication', 'electronic communication', and 'investigative or law enforcement officer' have the meanings given those terms in section 2510 of this title;

"(2) the terms 'encrypt' and 'encryption' refer to the scrambling of wire communications, electronic communications, or electronically stored information, using mathematical formulas or algorithms in order to preserve the confidentiality, integrity, or authenticity of, and prevent unauthorized recipients from accessing or altering, such communications or information;

"(3) 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; and

"(4) the term 'United States person' means—

"(A) any United States citizen;

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

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

"§ 2802. Assistance for law enforcement

"(a) NATIONAL ELECTRONIC TECHNOLOGIES CENTER.—

"(1) ESTABLISHMENT.—There is established in the Department of Justice a National Electronic Technologies Center (in this subsection referred to as the 'NET Center').

"(2) DIRECTOR.—The NET Center shall have a Director, who shall be appointed by the Attorney General.

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

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

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

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

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

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

"(i) reverse-steganography;

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

"(iii) de-multiplexing; and

"(F) to obtain information regarding the most current hardware, software, telecommunications, and other capabilities to understand how to access information transmitted across networks.

"(4) 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.

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

"(6) 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 subsection—

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

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

"(7) 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.

"(8) ADVISORY BOARD.—

"(A) ESTABLISHMENT.—There is established the Advisory Board of the Strategic NET Center for Excellence in Information Security (in this paragraph referred to as the 'Advisory Board'), which shall be comprised of members who have the qualifications described in subparagraph (B) and who are appointed by the Attorney General. The Attorney General shall appoint a chairman of the Advisory Board.

"(B) 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.

"(C) 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.

"(9) IMPLEMENTATION PLAN.—Within 2 months after the date of the enactment of the Security and Freedom Through Encryption (SAFE) Act, the Attorney General shall, 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—

"(A) 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 subsection;

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

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

"(b) FREEDOM OF USE.—Subject to section 2805, it shall be lawful for any person within any State, and for any United States person in a foreign country, to use any encryption, regardless of the encryption algorithm selected, encryption key length chosen, or implementation technique or medium used. No Federal or State law or regulation may condition the issuance of certificates of authentication or certificates of authority for any encryption product upon any escrowing or other sharing of private encryption keys, whether with private agents or government entities, or estab-

lish a licensing, labeling, or other regulatory scheme for any encryption product that requires key escrow as a condition of licensing or regulatory approval.

"§ 2803. Freedom to sell encryption

"Subject to section 2805, it shall be lawful for any person within any State to sell in interstate commerce any encryption, regardless of the encryption algorithm selected, encryption key length chosen, or implementation technique or medium used.

"§ 2804. Prohibition on mandatory key escrow

"(a) PROHIBITION.—No person in lawful possession of a key to encrypted communications or information may be required by Federal or State law to relinquish to another person control of that key.

"(b) EXCEPTION FOR ACCESS FOR LAW ENFORCEMENT PURPOSES.—Subsection (a) shall 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 effective date of this chapter, to gain access to encrypted communications or information.

"§ 2805. Unlawful use of encryption in furtherance of a criminal act

"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 10 years, or fined in the amount set forth in this title, or both; and

"(2) in the case of a second or subsequent offense under this section, shall be imprisoned for not more than 20 years, or fined in the amount set forth in this title, or both.

"§ 2806. Liability limitations

"No person shall be subject to civil or criminal liability for providing access to the plaintext of encrypted communications or electronic information to any law enforcement official or authorized government entity, pursuant to judicial process.".

(b) STUDY.—Within 6 months after the date of the enactment of this Act, the National Telecommunications and Information Administration shall conduct a study, and prepare and submit to the Congress and the President a report regarding such study, that—

(1) assesses the effect that establishment of a mandatory system for recovery of encryption keys for encrypted communications and information would have on—

(A) electronic commerce;
(B) data security;
(C) privacy in interstate commerce; and
(D) law enforcement authorities and activities; and

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

(c) CONFORMING AMENDMENT.—The table of chapters for part I of title 18, United States Code, is amended by inserting after the item relating to chapter 123 the following new item:

"125. Encrypted wire and electronic information ..... 2801".

SEC. 3. 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 thereof the following new subsection:

"(g) 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, 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) ITEMS NOT REQUIRING LICENSES.—No validated 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 software, including software with encryption capabilities—

"(i) that is generally available, as is, and is designed for installation by the purchaser; or

"(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

"(B) any computing device solely because it incorporates or employs in any form software (including software with encryption capabilities) exempted from any requirement for a validated license under subparagraph (A).

"(3) SOFTWARE WITH ENCRYPTION CAPABILITIES.—The Secretary shall authorize the export or reexport of software with encryption capabilities for nonmilitary end uses in any country to which exports of software of similar capability are permitted for use by financial institutions not controlled in fact by United States persons, unless there is substantial evidence that such software will be—

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

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

"(C) reexported without any authorization by the United States that may be required under this Act.

"(4) HARDWARE WITH ENCRYPTION CAPABILITIES.—The Secretary shall authorize the export or reexport of computer hardware with encryption capabilities if the Secretary determines that a product offering comparable security is commercially available outside the United States from a foreign supplier, without effective restrictions.

"(5) DEFINITIONS.—As used in this subsection—

"(A) the term 'encryption' means the scrambling of wire or electronic information using mathematical formulas or algorithms in order to preserve the confidentiality, integrity, or authenticity of, and prevent unauthorized recipients from accessing or altering, such information;

"(B) the term 'generally available' means, in the case of software (including software with encryption capabilities), software that is 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;

"(C) the term 'as is' means, in the case of software (including software with encryption capabilities), a software program that is not designed, developed, or tailored by the software publisher for specific purchasers, except that such purchasers may supply certain installation parameters needed by the software program to function properly with the purchaser's system and may customize the software program by choosing among options contained in the software program;

"(D) the term 'is designed for installation by the purchaser' means, in the case of software (including software with encryption capabilities) that—

"(i) the software publisher intends for the purchaser (including any licensee or transferee), who may not be the actual program user, to install the software program on a computing device and has supplied the necessary instructions to do so, except that the publisher may also provide telephone help line services for software installation, electronic transmission, or basic operations; and

"(ii) the software program is designed for installation by the purchaser without further substantial support by the supplier;

"(E) 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; and

"(F) the term 'computer hardware', when used in conjunction with information security, includes, but is not limited to, computer systems, equipment, application-specific assemblies, modules, and integrated circuits.".

(b) 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. 4. TREATMENT OF ENCRYPTION IN INTERSTATE AND FOREIGN COMMERCE.

(a) INQUIRY REGARDING IMPEDIMENTS TO TRADE.—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 unfair 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 of Commerce, in consultation with the Attorney General, 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 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.

(c) INTERNATIONAL AGREEMENTS.—

(1) REPORT TO PRESIDENT.—Upon the completion of the inquiry under subsection (a), the Secretary of Commerce 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.

(d) DEFINITIONS.—For purposes of this section, the following definitions shall apply:

(1) COMMUNICATION.—The term "communication" includes wire communication and electronic communication.

(2) DECRYPT; DECRYPTION.—The terms "decrypt" and "decryption" refer to the electronic retransformation of communications or electronically stored information that has been encrypted into the original form of the communication or information.

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

(4) ENCRYPT; ENCRYPTION.—The terms "encrypt" and "encryption" have the meanings given such terms in section 2801 of title 18, United States Code (as added by section 2 of this Act).

(5) ENCRYPTION PRODUCT.—The term "encryption product" means any product, software, or technology that can be used to encrypt and decrypt communications or electronic information and any product, software, or technology with encryption capabilities;

(6) WIRE COMMUNICATION.—The term "wire communication" has the meaning given such term in section 3 of the Communications Act of 1934 (47 U.S.C. 153).

SEC. 5. EFFECT ON LAW ENFORCEMENT ACTIVITIES.

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

PURPOSE AND SUMMARY

The growth of electronic commerce, electronic transactions, and interstate and foreign communications depends ultimately upon the

security and privacy of the information or data being transmitted. Encryption and the prolific use of encryption products are essential to facilitate this growth. Accordingly, the Committee on Commerce has an obligation and responsibility to ensure that the use of encryption technologies will have a positive impact on all electronic mediums, including the Internet, and all forms of existing and future electronic commerce. H.R. 695, the Security and Freedom Through Encryption (SAFE) Act, is intended to modernize the encryption policy of the United States. It is also intended to address law enforcement's and national security's needs as strong encryption products become more widely used.

In summary, H.R. 695, as amended by the Committee on Commerce, establishes a National Electronic Technologies Center (NET Center) to help Federal, State, and local law enforcement agencies obtain access to encrypted communications. H.R. 695 also states that it is lawful to use encryption products within the United States and requires a study assessing the impact that a mandatory key recovery system would have on, inter alia, electronic commerce. In addition, H.R. 695 prohibits any person from relinquishing an encryption key and provides penalties for using encryption products to conceal incriminating evidence. With respect to export law, H.R. 695 relaxes U.S. export policies by permitting mass-market encryption products to be exported under a general license exception. It also permits other computer hardware and software products to be exported subject to approval by the Secretary of Commerce. Finally, H.R. 695 requires the Secretary of Commerce to study domestic and foreign impediments to trade with respect to encryption products and requires the President to undertake negotiations with other countries as necessary to reduce impediments to U.S. encryption exports, as well as requiring the Attorney General to compile information regarding instances when law enforcement's efforts have been stymied because of the use of strong encryption products.

BACKGROUND AND NEED FOR LEGISLATION

Encryption is the commonly-used term to describe the use of cryptography to ensure the confidentiality of messages. Encryption products may be computer software, computer hardware, or another piece of equipment that has the capability to encode or decode messages. These products could 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 quadrillions of possible combinations. 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 products designed for non-military purposes.

As commercially-available encryption products have increased in strength over the years, the law enforcement community, led by the Federal Bureau of Investigations (FBI) and National Security Agency, has become increasingly concerned with the ability of

criminals, international terrorists, and certain countries to gain access to encryption products. Consequently, the Reagan, Bush, and Clinton Administrations have prohibited the export of encryption products with strengths greater than 40-bit key length to limit the proliferation of advanced encryption products that would affect their ability to protect the public safety. In general, a "key" is a form of information that is used in a mathematical formula, code, or algorithm to decrypt wire communications, electronic communications, or electronically stored information that has been encrypted. The Federal Government has never limited the use of encryption products domestically.

In 1996, the Administration eased the export restrictions and transferred control of export products from the Department of State to the Department of Commerce. The Department of Commerce's new regulations, which embody the Administration's current encryption export policies, can be summarized as follows:

There are no restrictions on the ability to buy, sell, manufacture, or distribute encryption products within the United States;

Encryption items up to 56-bit key length strength without a "key recovery system" will be permitted for export and re-export after a one-time review, if the exporter makes satisfactory commitments to build and/or market a key recovery system. This relaxation of controls expires on December 31, 1998. A key recovery system permits a person to hold and maintain sufficient decryption information to allow for the immediate decryption of the encrypted data or communications of another person for whom that information is held;

Weaker encryption products (40-bit key strength or less) or company proprietary software may be exported after a one-time review;

Controlled encryption items (such as those items with strengths greater than 56-bit length) may be exported after a one-time review if the items contain key-recovery technology;

Controlled encryption items used by banks and financial institutions are generally available for export regardless of whether key recovery is used; and

In general, there is a prohibition on exporting encryption items to Cuba, Iran, Iraq, Libya, North Korea, Syria, and Sudan.

The Committee on Commerce has been actively following and involved in the encryption debate this Congress. For example, in March 1997, Chairman Bliley and Representative White wrote letters to government leaders and the business community asking a series of questions on the Administration's current policies and on pending legislation. The letters and responses highlighted the two fundamental issues regarding encryption debate: (1) should domestic companies be permitted to export encryption products of any strength, thus increasing the availability of such products in the global market; and (2) should the United States impose any domestic restrictions on the use of encryption products to assist law enforcement's access to encrypted communications. In general, sound encryption policy must balance privacy interests with society's in-

terest to protect the public. To the greatest extent possible, it must also be based on free-market principles.

Regarding the arguments in the debate, the business community argues that current U.S. encryption policy harms domestic businesses abroad because they are forced to export weak encryption products that compete with stronger foreign encryption products. Many representatives of the business community also argue that the security of a strong encryption product is jeopardized if it contains a key-recoverable feature. In addition, the business community generally argues that the current policy may impose excessive costs on the industry to the extent they may be forced to develop costly, new key recovery products; manufacture two different products (one for the U.S. (strong) and one for abroad (weaker)); and/or be subject to a burdensome licensing process. Instead, they maintain that a key-recovery system should be developed only if there is market demand for such products.

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 key-recovery systems must be developed, not only to facilitate lawful searches and seizures, but to help users or employers in the event they lose the "key" to decrypt a message. They also argue that widespread use of strong encryption without key recovery would end the use of wiretapping as a tool for fighting crime and that lifting the export restrictions will undermine the Administration's effort to develop a global key-management infrastructure. In addition, they counter that most foreign countries view lifting the export restrictions as America's attempt to dominate world markets at the expense of other nation's national security, thereby forcing these countries to adopt import restrictions to keep American products out of their countries.

The existing encryption policy is 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 law enforcement in their ever increasing need to keep up with the latest technologies. In fact, the Committee finds that the current export rules place our domestic manufacturers of encryption products at a competitive disadvantage with our foreign counterparts without addressing the needs of law enforcement. Thus, at a minimum, current export law is not sustainable and potentially harmful to our domestic manufacturers.

At the same time, 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.

Consequently, legislation is needed to address the needs of law enforcement to access encrypted communications and to ease existing export restrictions that hamper domestic manufacturers of encryption products.

As reported by the Committee on Commerce, H.R. 695 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 to the future 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 the best way to help law enforcement protect public safety.

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. computer industry in a position where domestic companies can compete on a level playing field with their competitors in a global market. Moreover, H.R. 695 seeks to push for further relief for our manufacturers by directing the Department of Commerce to reduce foreign impediments to trade. The Committee has an obligation, through its jurisdiction over export promotion, to ensure that U.S. companies are not harmed in any way by unnecessary or unjust trade barriers.

Overall, the Committee finds that H.R. 695, as reported, strikes the appropriate balance between the needs of law enforcement and those of industry.

HEARINGS

The Subcommittee on Telecommunications, Trade, and Consumer Protection held a hearing on H.R. 695, the Security and Freedom Through Encryption (SAFE) Act, on September 4, 1997. The Subcommittee received testimony from the following witnesses: The Honorable Bob Goodlatte, U.S. Representative, Sixth District, Commonwealth of Virginia; The Honorable Zoe Lofgren, U.S. Representative, Sixteenth District, State of California; The Honorable William A. Reinsch, Under Secretary of Commerce for Export Administration, U.S. Department of Commerce; The Honorable Robert S. Litt, Deputy Assistant Attorney General, Criminal Division, U.S. Department of Justice; Mr. Stephen T. Walker, President and CEO, Trusted Information Systems, Inc.; Mr. Tom Parenty, Director, Data/Communications Security, Sybase, Inc.; Mr. Jerry Berman, Executive Director, Center for Democracy and Technology; and Mr. George A. Keyworth, Chairman, Progress and Freedom Foundation. Prior to hearing from the witnesses, The Honorable William P. Crowell, Deputy Director of the National Security Agency, provided an overview on encryption and described some of the common terms used in the encryption debate.

COMMITTEE CONSIDERATION

On September 24, 1997, the Committee on Commerce met in an open markup session to consider H.R. 695, the Security and Freedom Through Encryption (SAFE) Act. A unanimous consent request by Mr. Bliley to discharge the Subcommittee on Telecommunications, Trade, and Consumer Protection from further consideration and proceed to the immediate consideration of H.R. 695, as reported to the House by the Committee on the Judiciary, was agreed to without objection. The Committee ordered H.R. 695 reported to the House, amended, by a rollcall vote of 44 yeas to 6 nays.

ROLLCALL VOTES

Clause 2(l)(2)(B) of rule XI of the Rules of the House requires the Committee to list the recorded votes on the motion to report legislation and amendments thereto. The following are the recorded votes on the motion to report H.R. 695 and on amendments offered to the measure, including the names of those Members voting for and against.

COMMITTEE ON COMMERCE – 105TH CONGRESS
ROLL CALL VOTE #40

BILL: H.R. 695, Security and Freedom Through Encryption (SAFE) Act

AMENDMENT: An amendment by Mr. Oxley to the Markey Amendment to the Tauzin Amendment in the Nature of a Substitute, re: require encryption products made, sold, or imported to be recoverable.

DISPOSITION: NOT AGREED TO, by a roll call vote of 16 yeas to 35 nays.

REPRESENTATIVE	YEAS	NAYS	PRESENT	REPRESENTATIVE	YEAS	NAYS	PRESENT
Mr. Bliley		X		Mr. Dingell	X		
Mr. Tauzin		X		Mr. Waxman		X	
Mr. Oxley	X			Mr. Markey		X	
Mr. Billirakis	X			Mr. Hall		X	
Mr. Schaefer		X		Mr. Boucher		X	
Mr. Barton		X		Mr. Manton	X		
Mr. Hastert	X			Mr. Towns	X		
Mr. Upton	X			Mr. Pallone	X		
Mr. Stearns	X			Mr. Brown		X	
Mr. Paxon		X		Mr. Gordon		X	
Mr. Gillmor	X			Ms. Furse		X	
Mr. Klug	X			Mr. Deutsch		X	
Mr. Greenwood	X			Mr. Rush		X	
Mr. Crapo		X		Ms. Eshoo		X	
Mr. Cox		X		Mr. Klink		X	
Mr. Deal		X		Mr. Stupak	X		
Mr. Largent		X		Mr. Engel	X		
Mr. Burr		X		Mr. Sawyer		X	
Mr. Bilbray		X		Mr. Wynn		X	
Mr. Whitfield		X		Mr. Green		X	
Mr. Ganske	X			Ms. McCarthy		X	
Mr. Norwood		X		Mr. Strickland		X	
Mr. White		X		Ms. DeGette		X	
Mr. Coburn		X					
Mr. Lazio	X						
Mrs. Cubin		X					
Mr. Rogan		X					
Mr. Shimkus		X					

9/24/97

COMMITTEE ON COMMERCE – 105TH CONGRESS
ROLL CALL VOTE #41

BILL: H.R. 695, Security and Freedom Through Encryption (SAFE) Act

AMENDMENT: Amendment to the Tauzin Amendment in the Nature of a Substitute by Mr. Markey re: establishes a National Electronic Technologies Center (NET Center) to help Federal, State, and local law enforcement agencies obtain access to encrypted communications.

DISPOSITION: AGREED TO, by a roll call vote of 40 yeas to 11 nays.

REPRESENTATIVE	YEAS	NAYS	PRESENT	REPRESENTATIVE	YEAS	NAYS	PRESENT
Mr. Billey	X			Mr. Dingell		X	
Mr. Tauzin	X			Mr. Waxman	X		
Mr. Oxley		X		Mr. Markey	X		
Mr. Bilirakis		X		Mr. Hall	X		
Mr. Schaefer	X			Mr. Boucher	X		
Mr. Barton	X			Mr. Manton		X	
Mr. Hastert		X		Mr. Towns		X	
Mr. Upton	X			Mr. Pallone	X		
Mr. Stearns		X		Mr. Brown		X	
Mr. Paxon	X			Mr. Gordon	X		
Mr. Gillmor		X		Ms. Furse	X		
Mr. Klug	X			Mr. Deutsch	X		
Mr. Greenwood	X			Mr. Rush	X		
Mr. Crapo	X			Ms. Eshoo	X		
Mr. Cox	X			Mr. Klink	X		
Mr. Deal	X			Mr. Stupak	X		
Mr. Largent	X			Mr. Engel	X		
Mr. Burr	X			Mr. Sawyer	X		
Mr. Bilbray	X			Mr. Wynn	X		
Mr. Whitfield	X			Mr. Green	X		
Mr. Ganske		X		Ms. McCarthy	X		
Mr. Norwood	X			Mr. Strickland	X		
Mr. White	X			Ms. DeGette	X		
Mr. Coburn	X						
Mr. Lazio		X					
Mrs. Cubin	X						
Mr. Rogan	X						
Mr. Shimkus	X						

9/24/97

COMMITTEE ON COMMERCE -- 105TH CONGRESS
ROLL CALL VOTE #42

BILL: H.R. 695, Security and Freedom Through Encryption (SAFE) Act

MOTION: Motion by Mr. Bliley to order H.R. 695, reported to the House, amended.

DISPOSITION: AGREED TO, by a roll call vote of 44 yeas to 6 nays.

REPRESENTATIVE	YEAS	NAYS	PRESENT	REPRESENTATIVE	YEAS	NAYS	PRESENT
Mr. Bliley	X			Mr. Dingell		X	
Mr. Tauzin	X			Mr. Waxman			
Mr. Oxley		X		Mr. Markey	X		
Mr. Billirakis	X			Mr. Hall	X		
Mr. Schaefer	X			Mr. Boucher	X		
Mr. Barton	X			Mr. Manton		X	
Mr. Hastert		X		Mr. Towns	X		
Mr. Upton	X			Mr. Pallone	X		
Mr. Stearns	X			Mr. Brown		X	
Mr. Paxon	X			Mr. Gordon	X		
Mr. Gillmor	X			Ms. Furse	X		
Mr. Klug	X			Mr. Deutsch	X		
Mr. Greenwood	X			Mr. Rush	X		
Mr. Crapo	X			Ms. Eshoo	X		
Mr. Cox	X			Mr. Klink	X		
Mr. Deal	X			Mr. Stupak	X		
Mr. Largent	X			Mr. Engel	X		
Mr. Burr	X			Mr. Sawyer	X		
Mr. Bilbray	X			Mr. Wynn	X		
Mr. Whitfield	X			Mr. Green	X		
Mr. Ganske		X		Ms. McCarthy	X		
Mr. Norwood	X			Mr. Strickland	X		
Mr. White	X			Ms. DeGette	X		
Mr. Coburn	X						
Mr. Lazio	X						
Mrs. Cubin	X						
Mr. Rogan	X						
Mr. Shimkus	X						

9/24/97

COMMITTEE ON COMMERCE—105TH CONGRESS VOICE VOTES

Bill: H.R. 695, Security and Freedom Through Encryption (SAFE) Act

Amendment: Amendment in the Nature of a Substitute by Mr. Tauzin. (A unanimous consent request by Mr. Tauzin to have the Amendment in the Nature of a Substitute considered as base text for purposes of further amendment was agreed to without objection.)

Disposition: Agreed to, amended, by a voice vote.

Amendment: Amendment to the Tauzin Amendment in the Nature of a Substitute by Mr. Tauzin re: add a new section to direct the Secretary of Commerce to reduce interstate and foreign impediments to trade of encryption products and services.

Disposition: Agreed to, by a voice vote.

COMMITTEE OVERSIGHT FINDINGS

Pursuant to clause 2(l)(3)(a) of rule XI 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 AND OVERSIGHT

Pursuant to clause 2(l)(3)(D) of rule XI of the Rules of the House of Representatives, no oversight findings have been submitted to the Committee by the Committee on Government Reform and Oversight.

NEW BUDGET AUTHORITY AND TAX EXPENDITURES

In compliance with clause 2(l)(3)(B) of rule XI of the Rules of the House of Representatives, the Committee finds that H.R. 695, the Security and Freedom Through Encryption (SAFE) Act, would result in no new or increased budget 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 403 of the Congressional Budget Act of 1974.

CONGRESSIONAL BUDGET OFFICE ESTIMATE

Pursuant to clause 2(l)(3)(C) of rule XI of the Rules of the House of Representatives, the following is the cost estimate provided by the Congressional Budget Office pursuant to section 403 of the Congressional Budget Act of 1974:

U.S. CONGRESS,
CONGRESSIONAL BUDGET OFFICE,
Washington, DC, September 29, 1997.

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

If you wish further details on this estimate, we will be pleased to provide them. The CBO staff contacts are Rachel Forward and Mark Grabowicz (for Federal costs), Alyssa Trzeszkowski (for revenues), and Pepper Santalucia (for the impact on State, local, and tribal governments.

Sincerely,

JUNE E. O'NEILL, *Director.*

Enclosure.

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

Summary: H.R. 695 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 Bureau of Export Administration (BXA) in the Department of Commerce (DOC) from restricting the export of most nonmilitary encryption products. H.R. 695 would establish a National Electronic Technologies (NET) Center in the Department of Justice (DOJ) to provide assistance and information on encryption products to law enforcement officials and would require the Attorney General to maintain data on the instances in which encryption impedes or obstructs the ability of DOJ to enforce criminal laws. Finally, the bill would establish criminal penalties and fines for the use of encryption technologies to conceal incriminating information related to a felony.

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 $28 million over the 1998–2002 period. Spending by DOC and DOJ for activities required by H.R. 695 would total at least $33 million over the next five years. By comparison, CBO estimates that—under current policies—spending by BXA for reviewing the export of nonmilitary encryption products would total about $4.5 million over the same period. (Spending related to encryption exports by DOJ is negligible under current law.)

Enacting H.R. 695 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 or receipts would not be significant.

H.R. 695 contains no private-section mandates as defined in the Unfunded Mandates Reform Act of 1995 (UMRA). The bill contains intergovernmental mandates on state governments. CBO estimates, however, that states would not incur any costs to comply with the mandates.

Estimated cost to the Federal Government: Spending Subject to Appropriation—Under current policy, BXA would likely spend about $900,000 a year reviewing exports of encryption products. Assuming appropriation of the necessary amounts, CBO estimates that enacting H.R. 695 would lower BXA's encryption-related costs to about $500,000 a year. 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. 695 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. Thus, enacting H.R. 695 would reduce the costs to BXA to control the exports of nonmilitary encryption products.

H.R. 695 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 1998, assuming appropriation of the necessary amount.

H.R. 695 would establish within DOJ the NET Center, which generally 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 could depend on the extent to which service would be provided to the law enforcement community nationwide. Based on information from DOJ, we estimate that the minimum costs to fulfill the bill's requirements would be roughly $5 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, assuming appropriation of the necessary amounts.

Direct Spending and Revenues—Enacting H.R. 695 would affect direct spending and receipts by imposing criminal fines for encrypting incriminating information related to a felony. CBO estimates that collections from such fines are likely to be negligible, however, because the federal government would probably not pursue many cases under the bill. Any such collections would be recorded in the budget as governmental receipts, or revenues. They would be deposited in the Crime Victims Fund and spent the following year. Because the increase in direct spending would be the same as the amount of fines collected with a one-year lag, 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 the work of the office. CBO expects that any contributions (recorded in the budget as revenues) 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.

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

Pay-as-you-go-considerations: Section 252 of the Balanced Budget and Emergency Control Act of 1985 sets up pay-as-you-go procedures for legislation affecting direct spending or receipts. H.R. 695 would affect direct spending and receipts 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. 695 would prohibit states from requiring anyone in lawful possession of an encryption key to make that key available to another person or entity. The bill would also prohibit states from conditioning the issuance of certificates of authenticity or certificates of authority for encryption products on the sharing of encryption keys Finally, the bill would prohibit states from establishing licensing, labeling, or other regulatory schemes for encryption products that would require the sharing of encryption keys. These prohibitions would be intergovernmental mandates as defined in UMRA. However, states would bear no costs as a result of these mandates, because none currently have laws that would violate these provisions of the bill.

H.R. 695 would also establish a center in the Justice Department that would provide information and assistance regarding decryption techniques to federal, state, and local law enforcement authorities.

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

Previous CBO estimates: CBO provided cost estimates for H.R. 695 as ordered reported by the House Committee on the Judiciary on May 14, 1997, by the House Committee on International Relations on July 22, 1997, by the House Committee on National Security on September 9, 1997, and by the House Committee on Intelligence on September 11, 1997. Assuming appropriation of the necessary amounts, CBO estimates that costs over the 1998–2002 period would total between $5 million and $7 million for the Judiciary Committee's version, about $2.2 million for the International Relations Committee's version, about $4.5 million for the National Security Committee's version, and between $9 million and $11.6 million for the Intelligence Committee's version. In comparison, CBO estimates that enacting this version of the bill would cost at least $33 million over the 1998–2002 period and that spending under current policies would total $44.5 million over the same period.

Estimate prepared by: Federal costs: Rachel Forward and Mark Grabowicz; Revenues: Alyssa Trzeszkowski; Impact on State, local, and tribal governments: Pepper Santalucia.

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

H.R. 695 creates an Advisory Board of the Strategic NET Center for Excellence in Information Security, which is intended to advise the Federal Government on new technologies relating to encryption.

CONSTITUTIONAL AUTHORITY STATEMENT

Pursuant to clause 2(l)(4) of rule XI 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 provides that H.R. 695 may be cited as the "Security and Freedom Through Encryption (SAFE) Act."

SECTION 2. SALE AND USE OF ENCRYPTION

Subsection 2(a) of H.R. 695 creates a new chapter 125 in title 18 of the United States Code. This chapter 125 would include new sections 2801–012.

Section 2801. Definitions

New section 2801 provides for definitions of terms to be used in the chapter. Many of the definitions used are explicitly taken from the definitions in the existing Federal wiretap statute, 18 U.S.C. Sec. 2510 et seq. Several new definitions are added, however, including "encrypt" and "encryption," which generally refer to the encoding of a communication using mathematical formulas in order to preserve the confidentiality of such communication.

Section 2802. Assistance for law enforcement

New section 2802 contains several subsections regarding domestic encryption issues. Subsection 2802(a) establishes within the Department of Justice 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 Attorney General 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 Attorney General 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.

In addition, subsection 2802(a) creates an Advisory Board of the Strategic NET Center for Excellence in Information Security, which is intended to advise the government on new technologies relating to encryption. The Attorney General 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.

Subsection 2802(b) clarifies that it is lawful for any person in the United States to use any encryption product, regardless of the encryption algorithm selected, key length chosen, implementation technique used, or medium used. This subsection also prohibits the adoption of Federal or State law or regulation that would condition the issuance of certificates of authentication for any encryption product upon any escrowing or other sharing of private encryption keys, whether the escrowing is done with private agents or government entities. Domestic laws or regulations also could not establish a licensing, labeling, or other regulatory scheme for any encryption

product that requires key escrow as a condition of licensing or regulatory approval.

Section 2803. Freedom to sell encryption

New section 2803 states that it is legal for any person in the United States to sell in interstate commerce encryption products using any form of encryption regardless of the algorithm, key length, or technique used. The Committee intends that sections 2802 and 2803 should be read as limitations on government power. They should not be read as overriding otherwise lawful employer policies concerning employee use of the employer's computer system, nor as limiting the employer's otherwise lawful means for remedying violations of those policies.

Section 2804. Prohibition on mandatory key escrow

New section 2804 states that no person in lawful possession of a key used to encrypt or decrypt a communication or information can be required by Federal or State law to relinquish control of that key to another person. This section is meant to be consistent with subsection 2802(b) regarding limitations on the escrowing of keys. An exception is provided, however, for law enforcement. That is, a law enforcement officer or any member of the intelligence community acting pursuant to lawful authority may require a party to release a key in order to gain access to encrypted communications or information.

Section 2805. Unlawful use of encryption in furtherance of a criminal act

New section 2805 makes it a crime to encrypt incriminating communications 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 10 years, or both. Second and subsequent offenses may result in a fine, imprisonment of not more than 20 years, or both.

Section 2806. Liability limitations

New section 2806 protects persons from being subject to criminal or civil liability if they provide access to the plaintext of an encrypted communications or electronic information for the benefit of any law enforcement official or authorized government entity, so long as these entities operate through the appropriate judicial process.

Subsection 2(b) requires the National Telecommunications and Information Administration of the Department of Commerce to conduct a study and prepare and submit an encryption report to the Congress and the President. The report must determine what effect a mandatory key recovery system would have on electronic commerce, data security, privacy, and law enforcement activities. The report must also assess other possible methods for providing access to encrypted communications and information to further law enforcement activities.

Subsection 2(c) of H.R. 695 provides for a conforming amendment to the table of chapters in title 18, United States Code.

SECTION 3. EXPORTS OF ENCRYPTION

Subsection 3(a) of H.R. 695 amends the Export Administration Act of 1979 by creating a new subsection (g) to 50 U.S.C. App. Sec. 2416. New subsection (g)(1) would place all encryption products, except those specifically designed or modified for military use, under the exclusive jurisdiction of the Secretary of Commerce (the Secretary).

New subsection (g)(2) allows encryption products, such as encryption software and computing devices that include encryption software, that are generally available or in the public domain, such as mass-market products, to be exported pursuant to a general license exception. New subsections (g)(3) and (g)(4) permit the export of encryption products that are not generally considered mass-market products and consequently, require a license for export. The Secretary retains the authority to disapprove a license request for the export of software if there is substantial evidence that it will be put to military or terrorist uses or that it will be re-exported without U.S. authorization. New subsection (g)(5) provides definitions.

Subsection 3(b) of H.R. 695 provides that for purposes of carrying out the amendment made by subsection 3(a), the Export Administration Act shall be deemed to be in effect. This statement is necessary because Congress allowed the Export Administration Act to lapse in 1994. To date, it has not been renewed, and its policies have been continued by Executive Order.

SECTION 4. TREATMENT OF ENCRYPTION IN INTERSTATE AND FOREIGN COMMERCE

Section 4 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 on Commerce intends to promote robust participation by U.S. firms in the development of global electronic commerce.

Subsection 4(a) requires the Secretary to complete an inquiry within 180 days of the enactment of this Act to identity 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 4(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 4(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 shall submit a report to the President on his or her findings. The report must in-

clude a determination by the Secretary on what impediments may require international negotiation to reduce.

Subsection 4(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 4(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 his efforts on encryption not later than December 31, 2000.

Subsection 4(d) provides definitions.

SECTION 5. EFFECT ON LAW ENFORCEMENT ACTIVITIES

Subsection 5(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 5(b) requires that the Attorney General shall make the information compiled under subsection 5(a), including an unclassified summary, available to Members of Congress upon request.

CHANGES IN EXISTING LAW MADE BY THE BILL, AS REPORTED

In compliance with clause 3 of rule XIII of the Rules of the House of Representatives, changes in existing law made by the bill, as reported, are shown as follows (new matter is printed in italics and existing law in which no change is proposed is shown in roman):

TITLE 18, UNITED STATES CODE

* * * * * * *

PART I—CRIMES

CHAPTER 125—ENCRYPTED WIRE AND ELECTRONIC INFORMATION

§2801. Definitions

As used in this chapter—

(1) the terms "person", "State", "wire communication", "electronic communication", and "investigative or law enforcement officer" have the meanings given those terms in section 2510 of this title;

(2) the terms "encrypt" and "encryption" refer to the scrambling of wire communications, electronic communications, or electronically stored information, using mathematical formulas or algorithms in order to preserve the confidentiality, integrity, or authenticity of, and prevent unauthorized recipients from accessing or altering, such communications or information;

(3) 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; and

(4) the term "United States person" means—

(A) any United States citizen;

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

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

§2802. Assistance for law enforcement

(a) NATIONAL ELECTRONIC TECHNOLOGIES CENTER.—

(1) ESTABLISHMENT.—There is established in the Department of Justice a National Electronic Technologies Center (in this subsection referred to as the "NET Center").

(2) DIRECTOR.—The NET Center shall have a Director, who shall be appointed by the Attorney General.

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

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

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

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

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

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

(i) reverse-steganography;

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

(iii) de-multiplexing; and

(F) to obtain information regarding the most current hardware, software, telecommunications, and other capabilities to understand how to access information transmitted across networks.

(4) 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.

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

(6) 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 subsection—

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

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

(7) 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.

(8) ADVISORY BOARD.—

(A) ESTABLISHMENT.—There is established the Advisory Board of the Strategic NET Center for Excellence in Information Security (in this paragraph referred to as the "Advisory Board"), which shall be comprised of members who have the qualifications described in subparagraph (B) and who are appointed by the Attorney General. The Attorney General shall appoint a chairman of the Advisory Board.

(B) 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.

(C) 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.

(9) IMPLEMENTATION PLAN.—Within 2 months after the date of the enactment of the Security and Freedom Through Encryption (SAFE) Act, the Attorney General shall, 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—

(A) 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 subsection;

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

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

(b) FREEDOM OF USE.—Subject to section 2805, it shall be lawful for any person within any State, and for any United States person in a foreign country, to use any encryption, regardless of the encryption algorithm selected, encryption key length chosen, or implementation technique or medium used. No Federal or State law or regulation may condition the issuance of certificates of authentication or certificates of authority for any encryption product upon any escrowing or other sharing of private encryption keys, whether with private agents or government entities, or establish a licensing, labeling, or other regulatory scheme for any encryption product that requires key escrow as a condition of licensing or regulatory approval.

§2803. Freedom to sell encryption

Subject to section 2805, it shall be lawful for any person within any State to sell in interstate commerce any encryption, regardless of the encryption algorithm selected, encryption key length chosen, or implementation technique or medium used.

§2804. Prohibition on mandatory key escrow

(a) PROHIBITION.—No person in lawful possession of a key to encrypted communications or information may be required by Federal or State law to relinquish to another person control of that key.

(b) EXCEPTION FOR ACCESS FOR LAW ENFORCEMENT PURPOSES.—Subsection (a) shall 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 effective date of this chapter, to gain access to encrypted communications or information.

§2805. Unlawful use of encryption in furtherance of a criminal act

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 10 years, or fined in the amount set forth in this title, or both; and

(2) in the case of a second or subsequent offense under this section, shall be imprisoned for not more than 20 years, or fined in the amount set forth in this title, or both.

§2806. Liability limitations

No person shall be subject to civil or criminal liability for providing access to the plaintext of encrypted communications or electronic information to any law enforcement official or authorized government entity, pursuant to judicial process.

* * * * * * *

SECTION 17 OF THE EXPORT ADMINISTRATION ACT OF 1979

EFFECT ON OTHER ACTS

SEC. 17. (a) * * *

* * * * * * *

(g) 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, 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) ITEMS NOT REQUIRING LICENSES.—No validated 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 software, including software with encryption capabilities—

(i) that is generally available, as is, and is designed for installation by the purchaser; or

(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

(B) any computing device solely because it incorporates or employs in any form software (including software with encryption capabilities) exempted from any requirement for a validated license under subparagraph (A).

(3) SOFTWARE WITH ENCRYPTION CAPABILITIES.—The Secretary shall authorize the export or reexport of software with encryption capabilities for nonmilitary end uses in any country to which exports of software of similar capability are permitted for use by financial institutions not controlled in fact by United States persons, unless there is substantial evidence that such software will be—

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

(B) modified for military or terrorist end use; or

(C) reexported without any authorization by the United States that may be required under this Act.

(4) HARDWARE WITH ENCRYPTION CAPABILITIES.—The Secretary shall authorize the export or reexport of computer hardware with encryption capabilities if the Secretary determines that a product offering comparable security is commercially available outside the United States from a foreign supplier, without effective restrictions.

(5) DEFINITIONS.—As used in this subsection—

(A) the term "encryption" means the scrambling of wire or electronic information using mathematical formulas or algorithms in order to preserve the confidentiality, integrity, or authenticity of, and prevent unauthorized recipients from accessing or altering, such information;

(B) the term "generally available" means, in the case of software (including software with encryption capabilities), software that is 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;

(C) the term "as is" means, in the case of software (including software with encryption capabilities), a software program that is not designed, developed, or tailored by the software publisher for specific purchasers, except that such purchasers may supply certain installation parameters needed by the software program to function properly with the purchaser's system and may customize the software program by choosing among options contained in the software program;

(D) the term "is designed for installation by the purchaser" means, in the case of software (including software with encryption capabilities) that—

(i) the software publisher intends for the purchaser (including any licensee or transferee), who may not be the actual program user, to install the software program on a computing device and has supplied the necessary instructions to do so, except that the publisher may also provide telephone help line services for software installation, electronic transmission, or basic operations; and

(ii) the software program is designed for installation by the purchaser without further substantial support by the supplier;

(E) 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; and

(F) the term "computer hardware", when used in conjunction with information security, includes, but is not limited to, computer systems, equipment, application-specific assemblies, modules, and integrated circuits.

DISSENTING VIEWS

While we are supportive of the stated goals of H.R. 695, particularly with respect to the promotion of U.S. technology exports, we have serious reservations about the bill as reported. It is our view that the provisions ultimately agreed to by the Committee with regard to the technological requirements of law enforcement and national security agencies are thoroughly inadequate to the missions at hand.

We do not question the importance of encryption technology for purposes of protecting electronic commerce, consumer privacy, and proprietary information, nor do we doubt the value of enhancing U.S. access to foreign markets for these products and services. We have great confidence in the ability of American firms to develop the most impenetrable encryption products in the world and market them globally.

Indeed, it is our very faith in the technological prowess of U.S. companies which leads us to conclude that authentic law enforcement and national security safeguards must be included in this legislation. It must be recognized that the proliferation of advanced encryption technology poses a dire threat to U.S. anti-crime, anti-terrorism, and counter-espionage efforts. To fail to address this reality is to fail in or solemn responsibility to protect the lives and safety of the citizens of this country.

Powerful encryption, in criminal hands or in the hands of enemies of the United States, can be turned to ill purposes with devastating consequences for members of a free society. An outlaw organization with the ability to communicate and store data without fear of detection is a significantly more dangerous entity. Organized crime syndicates, drug cartels, pedophile rings and terrorist organizations have already begun to utilize encryption technology to conceal their activities from investigatory agencies.

It is our opinion that an updated U.S. encryption policy must allow for law enforcement and security agency access to the unscrambled text of encrypted communications and data, pursuant to legal authorization. We wish to clarify that we do not seek any additional authority for government agencies. We merely seek to ensure that police departments and security agencies will continue to have intelligible access to evidence to which they are legally entitled.

In the context of H.R. 695, this means that encryption products and services must be made recoverable. There is no other way to ensure timely access to encrypted evidence. Timely recovery is crucial in the investigation and prevention of crime and acts of terror; the bill as reported will not achieve this. Claims to the contrary, unfortunately, are false.

Included with these views are letters submitted by organizations and individuals whose sentiments on these matters comport with our own.

THOMAS J. MANTON.
J. DENNIS HASTERT.
MICHAEL G. OXLEY.
GREG GANSKE.

U.S. DEPARTMENT OF JUSTICE,
FEDERAL BUREAU OF INVESTIGATION,
Washington, DC, September 24, 1997.

Hon. THOMAS J. BLILEY, Jr.
Chairman, Committee on Commerce,
Rayburn House Office Building, Washington, DC.

DEAR MR. CHAIRMAN: We are writing you today on behalf of the entire law enforcement community to continue to urge you and the Members of the House Commerce Committee to support the Oxley/Manton Amendment to H.R. 695 during your Committee's mark-up of the bill today.

In addition, we are aware that Congressmen Markey and White plan to offer an alternative amendment to the Oxley/Manton Amendment during the mark-up that has been represented to meet law enforcement's decryption needs by creating a "National Electronic Technologies Center" to foster the "exchange of information and expertise" between government and industry. Let us assure you that the adoption of the Markey/White Amendment in lieu of the Oxley/Manton Amendment will not address the law enforcement and public safety issues we have raised and would serve to provide an illusion and false sense of security to the American people that law enforcement's public safety needs in this area have been effectively addressed. In reality the adoption of the Markey/White Amendment will actually continue to allow for the proliferation of unbreakable encryption products for use by the general public regardless of their adverse impact on public safety and national security.

The exchange of ideas between government and industry, which is the purpose of the center, is already occurring and has been for some time. The problem remains that absent an approach like Oxley/Manton, no technical solution for law enforcement is foreseeable. NSA agrees with our assessment. Having a central point of information and expertise might be helpful for sharing what is known but it will not solve the problem. Neither will enhanced criminal penalties.

Law enforcement continues to support the adoption of a balanced encryption policy, one that meets the needs of industry for robust encryption to protect sensitive information and the privacy of communications while at the same time meeting law enforcement's immediate decryption needs to protect public safety when such robust encryption products are used to protect serious criminal activity. Law enforcement is in unanimous agreement that the widespread availability and use of unbreakable robust encryption products for use in the United States will ultimately devastate our ability to protect American citizens from violent criminals, international drug

lords and prevent acts of terrorism directed at innocent Americans. It is for this reason that we are calling for a balanced solution to this problem. We believe that the provisions of the Oxley/Manton Amendment strike that balance and we urge your support for its adoption during today's mark-up.

Sincerely yours,

THOMAS CONSTANTINE,
Administrator, Drug Enforcement Administration.
RAYMOND W. KELLY,
Undersecretary for Enforcement, U.S. Department of the Treasury.
LOUIS J. FREEH,
Director.

NATIONAL SHERIFFS' ASSOCIATION,
Alexandria, VA, September 23, 1997.

Hon. THOMAS J. BLILEY, Jr.
Chairman, Committee on Commerce,
Rayburn House Office Building, Washington, DC.

DEAR MR. CHAIRMAN: I am writing to you today to urge you to support the Oxley Amendment to H.R. 695, the Security and Freedom Through Encryption Act. Without this amendment, H.R. 695 fails to protect the needs of law enforcement.

As you know, the access to intercepted communications or data when lawful authority exists is a fundamental tool that law enforcement employs in the fight against crime. Representative Oxley's amendment preserves that tool and enables law enforcement to thwart sophisticated criminal intentions. Criminals working with encryption technology can render traditional electronic surveillance methods obsolete and investigations are crippled without the ability to break the code. Meaningful encryption legislation has to ensure that law enforcement can gain timely access to the plaintext of encrypted conversations and information by established legal procedures.

The National Sheriffs' Association supports the actions taken by the Committee on National Security and the Permanent Select Committee on Intelligence to give authorities a tool to use against terrorists and other criminals who want to hide information. Without adequate safeguards, H.R. 695 will allow the use of powerful encryption, which will deprive law enforcement of the ability to ensure public safety and create a haven for the computer literate criminal.

Thank you for your consideration and we look forward to working with you to develop sound national policy on encryption. If I can provide you with any additional information, please do not hesitate to call on me at the National Sheriffs' Association at 1–800–424–7827.

Sincerely,

FRED W. SCORALICK, *President.*

NATIONAL DISTRICT ATTORNEYS ASSOCIATION,
Alexandria, VA, September 19, 1997.

Hon. MICHAEL G. OXLEY,
Rayburn House Office Building,
Washington, DC.

DEAR CONGRESSMAN OXLEY: The National District Attorneys Association has, and continues to oppose H.R. 695, the "Security and Freedom Through Encryption (SAFE) Act," as introduced and now before the Committee for review. As local prosecutors, we are extremely concerned about the serious threat posed by the use of robust encryption products that do not allow for court approved law enforcement access and timely decryption that has been encrypted to carry out criminal activity (court authorized wiretaps or court authorized search and seizure). We do support a balanced encryption policy that satisfies both the commercial needs of industry for robust encryption while at the same time satisfying law enforcement's public safety needs. The Amendment offered by you and Mr. Manton achieves this balance.

At the onset, we need to make perfectly clear, both to the Congress and to the American people that we seek no new authorities to intrude on Constitutionally protected rights of privacy nor do we seek any new authority to search for and seize evidence. Supporters of an unfettered encryption policy have made much of a fear for abuse of police powers and have lead many to believe that a decryption requirement will lead to random eavesdropping by police on our communications. This is far from the truth. Law enforcement does not seek any new authorities; we only seek the technological capability to preserve the current authority.

At Federal, State and local levels of law enforcement there are strictly observed sets of judicial and administrative requirements that must be adhered to obtain a judicial authorization to intercept a communication and to continue such interceptions. Among these requirements must be a showing that there is probable cause to believe that criminal enterprise is on going and that all other means of obtaining evidence are to no avail. When a judge does authorize an interception there is frequently a requirement that the authorization must be reviewed periodically by the judge and there is always the mandate that any communications pertaining to criminal activity may not be monitored.

We all recognize that encryption technology can be extremely beneficial when used legitimately to protect commercially sensitive information and private communications. The potential use, however, of such encryption products by criminals and terrorists to conceal their criminal communications and information from law enforcement poses an extremely serious threat to the public safety of our country.

The introduction of digitally-based telecommunications technologies, as well as the widespread use of computers and computer networks having encryption capabilities, is facilitating the development and production of affordable and robust encryption products for the private sector. American industrial concerns are not misplaced in desiring to enhance markets for their products, but this must never be accomplished at the expense of the lives and safety of the American people.

We are obligated, in the interests of our communities to oppose any efforts that endanger the people we have sworn to protect. Your amendment is an appropriate legislative solution to this complex problem in addressing both the needs of industry while at the same time satisfying the requirements of law enforcement as they pertain to protecting the American people. We most strongly urge the members of the Commerce Committee to support the Oxley/Manton Amendment.

Sincerely,

WILLIAM L. MURPHY, *President.*

NATIONAL DISTRICT ATTORNEYS ASSOCIATION

RESOLUTION—ENCRYPTION

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

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

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

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

Whereas, law enforcement has found that strong, key recovery encryption products and services are clearly the best way, and perhaps the only way, to achieve both the goals of industry and law enforcement; and

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

Be it resolved, that the National District Attorneys Association supports and encourages the development and adoption of a balanced encryption policy that encourages the development, sale, and use of key recovery encryption products and services, both domestically and abroad. We believe that this approach represents a policy that appropriately addresses both the commercial needs of industry

while at the same time satisfying law enforcement's public safety needs.

Adopted by the Board of Directors, November 16, 1996, Naples, Florida.

INTERNATIONAL ASSOCIATION OF CHIEFS OF POLICE,
Alexandria, VA, September 22, 1997.

Hon. MICHAEL G. OXLEY,
Rayburn House Office Building, House of Representatives, Washington, DC.

DEAR REPRESENTATIVE OXLEY: On behalf of the International Association of Chiefs of Police (IACP), I am writing to express our *strong support for your amendment to H.R. 695,* the Security and Freedom though Encryption (SAFE) Act. Your amendment, by requiring that no encryption technology be sold unless it contains features that would provide for immediate access no encrypted information, protects the ability of law enforcement agencies to perform court authorized electronic surveillance and the search and seizure of information stored in computers.

Throughout the debate on encryption legislation, IACP has stressed that need for provisions that would provide law enforcement with the ability to gain timely access to encrypted conversations and information. In its current form, H.R. 695 *does not* meet this standard. The passage of H.R. 695, without the adoption of the Oxley/Manton amendment, would severely weaken the ability of law enforcement to combat society's most dangerous criminals.

Thank you for your leadership on this issue of vital importance to law enforcement. If IACP can be of further assistance on this issue, please call IACP's Legislative Department at 703/836–6767 ext. 211.

Sincerely,

DARRELL L. SANDERS, *President.*

INTERNATIONAL ASSOCIATION OF CHIEFS OF POLICE,
Alexandria, VA, September 24, 1997.

DEAR COMMERCE COMMITTEE MEMBER: It is the understanding of the International Association of Chiefs of Police (IACP) that an amendment may be offered at today's mark-up of H.R. 695 that would call for the establishment of a commission to study the issue of law enforcement access to encrypted information. IACP is strongly opposed to any amendment that would delay providing law enforcement with access to encrypted criminal information. Any delay is a victory for those elements in society who wish to use encryption technology for criminal purposes.

IACP believes that action must be taken immediately to prevent the further proliferation of inaccessible encryption technology. The establishment of a commission will serve no purpose other than to exacerbate an already troubling situation facing law enforcement.

IACP strongly supports the Oxley/Manton Amendment. The Oxley/Manton Amendment, by requiring that no encryption technology be sold unless it contains features that provide for immediate access to information encrypted in the furtherance of criminal

activity, protects the ability of law enforcement agencies to perform court authorized electronic surveillance and the search and seizure of information stored in computers.

Throughout the debate on encryption legislation, IACP has stressed that need for provisions that would provide law enforcement with the ability to gain timely access to encrypted conversations and information that threaten public safety. In its current form, H.R. 695 does not meet this standard. The passage of H.R. 695, without the adoption of the Oxley/Manton amendment would severely weaken the ability of law enforcement to combat society's most dangerous criminals. Therefore, IACP urges you to support the Oxley/Manton amendment when H.R. 695 is considered by the House Commerce Committee.

Once again, IACP urges you to oppose any attempt to delay law enforcement access to encrypted information and to support the Oxley/Manton Amendment

Thank you for your support.

Sincerely,

DARRELL L. SANDERS, *President.*

MAJOR CITIES CHIEFS,
September 23, 1997.

Hon. MICHAEL G. OXLEY,
House of Representatives, Rayburn House Office Building, Washington, DC.

DEAR CONGRESSMAN OXLEY: The Major Cities Chiefs, an association of police executives representing 48 of the nation's largest jurisdictions, strongly supports the proposed Oxley/Manton amendments to H.R. 695. These amendments, which are scheduled to be considered by the Commerce Committee this week, would require both manufacturers of encryption devices and purveyors of encryption services to include features that would allow law enforcement access to encrypted information being used for illegal purposes.

Essentially, these amendments are intended to protect the limited, judicially sanctioned wiretap privileges already in effect for law enforcement agencies. They are not intended to enlarge in any way the scope of these privileges. Without these amendments, a criminal suspect could avoid an otherwise-legal wiretap merely by using an encrypted form of communication. The legality of a wiretap should be based on the evidence against a suspect, not on the form of communication the suspect uses.

Pursuant to these amendments, the Attorney General of the United States would be required to establish a rulemaking procedure within one year of their enactment. This would allow due consideration for he many legitimate uses of encryption. However, we must not compromise a law enforcement tool which has proved invaluable against major drug trafficking operations and other forms of organized crime.

Sincerely,

MATT L. RODRIGUEZ, *Chairman.*

September 23, 1997.

Hon. MICHAEL G. OXLEY,
Committee on Commerce, Rayburn H.O.B.,
Washington, DC.

DEAR MIKE: As your committee considers the Goodlatte encryption bill I would request that you support the Oxley/Manton Amendment.

The Goodlatte bill (H.R. 695) was drafted by and for the software industry at the expense of the national security and public safety needs of the American people.

In order to protect national security and public safety, I would ask that you support the Manton/Oxley amendment which would require the crucial key recovery language similar to the provisions adopted by the Intelligence Committee. If this language is not incorporated into the bill, as the Chairman of the House Rules Committee I will not move the bill to the House floor!

Thank your for your time and courtesy. Please contact me if you have any questions regarding this matter.

Sincerely,

GERALD B.H. SOLOMON, *Member of Congress.*

ILLINOIS ASSOCIATION OF CHIEFS OF POLICE,
Springfield, IL, September 23, 1997.

Hon. J. DENNIS HASTERT,
U.S. Representative, 14th District—Yorkville, IL,
Rayburn House Office Building, Washington, DC.

DEAR CONGRESSMAN HASTERT: On Thursday, September 25, 1997, the Committee on Commerce will hear legislation regarding encryption of electronically stored information. The Illinois Association of Chiefs of Police membership strongly urges you to vote for the Oxley/Manton Amendment which would allow for the manufacture of encryption products that include features accessible by lawful court ordered interceptions of wire and electronic communications. Such ability is absolutely necessary in this day of international and domestic terrorism, espionage and kidnapping.

On behalf of the membership, I thank you in advance for your support.

Very truly yours,

GEORGE F. KOERTGE, *Executive Director.*

CALIFORNIA PEACE OFFICERS' ASSOCIATION,
Sacramento, CA, September 19, 1997.

Hon. MICHAEL G. OXLEY,
Member, House of Representatives,
Rayburn House Office Building, Washington, DC.

Re H.R. 695.

DEAR CONGRESSMAN OXLEY: The House Commerce Committee is scheduled to soon hold a mark-up concerning Congressman Goodlatte's Encryption Bill (H.R. 695). As currently drafted, this bill does not address law enforcement's public safety concerns and needs regarding encryption. Your plan to propose an amendment

requiring manufacturers of encryption procedures in the United States to include features that would allow for immediate access to the plaintext of encrypted data should these products be used for illegal purposes is sincerely appreciated. The Federal Bureau of Investigation needs such a provision to fulfill their criminal investigative mission. Law enforcement agencies can not afford to allow modern technology to outdistance their ability to combat sophisticated criminal enterprises.

The California Peace Officers' Association supports your proposed amendment. Please feel free to include this letter in any official record of support that you may deem appropriate.

Very truly yours,

GREG COWART, *President.*

FLORIDA DEPARTMENT OF LAW ENFORCEMENT,
Tallahassee, FL, September 24, 1997.

Congressman MICHAEL OXLEY,
Rayburn House Office Building,
Washington, DC.

Re H.R. 695 ("Security and Freedom Through Encryption {SAFE} Act")

DEAR CONGRESSMAN OXLEY: Attached is a copy of a letter I have sent this morning to Congressman Tom Bliley, Chairman of the House Committee on Commerce supporting your proposed amendment to H.R. 695. The ability of law enforcement to decrypt encrypted communications must be assured in order to help law enforcement remain effective as we deal with the "age of encryption."

Your position statement found at your Internet site does an excellent job of identifying the problem and stressing law enforcement's need for decryption. Given the pending 3:30 p.m. "markup" on H.R. 695 this afternoon, I will not expand upon my comments as noted on the attached letter. Suffice it to say that if Congress does not provide for the decryption as needed, the scales of justice will be tilted significantly in favor of the criminal element.

Please do not hesitate to contact me at (850) 488–8771 should you desire additional comment or information from this Department.

Sincerely,

JAMES T. MOORE, *Commissioner.*

FLORIDA DEPARTMENT OF LAW ENFORCEMENT,
Tallahassee, FL, September 24, 1997.

Congressman TOM BLILEY,
Chairman, Committee on Commerce, Rayburn House Office Building, Washington, DC.

Re "Markup" at 3:30 p.m. today and H.R. 695

DEAR CHAIRMAN BLILEY: As Executive Director of the Florida Department of Law Enforcement, I am responsible for assuring that our investigations of organized criminal activity, be it drug-trafficking, money laundering, domestic terrorism, or predatory sexual

conduct, be conducted legally and with effort focused upon bringing those involved in such conduct to justice.

Congress, and the legislature of the State of Florida, have both recognized that law enforcement must have the ability to intercept communications of criminals in order to penetrate their criminal enterprises and develop the evidence essential to obtaining a conviction. Both federal and Florida state law currently authorize court-ordered interceptions of wire, oral or electronic communications. The process to obtain such court orders establishes a high level of law enforcement justification, including probable cause to believe a crime has been committed and that the communications will be evidence of the crime, as well as requiring a showing that other less-intrusive investigative techniques have been exhausted or will not produce the necessary evidence. Indeed, the current law has reached a good balance between privacy protections and the need for law enforcement to have the tools it must use to effectively fight crime.

Unless the H.R. 695 (the "Security and Freedom Through Encryption (SAFE) Act") is modified to provide law enforcement access to encrypted materials when law enforcement has obtained court authorization to do so, the ability of law enforcement at the federal and state level to effectively investigate organized criminal enterprises and activity will be severely damaged. Encryption is readily available today. Our Department's own experience with encrypted computer evidence is that, absent having access to encryption codes to "break" encrypted material, we can decypher only a very small portion of encrypted material. That which remains encrypted cannot be used as evidence against the criminals utilizing the encryption.

Congressmen Oxley and Manton have offered an amendment to H.R. 695 that will be considered by your Committee today which will allow real time decryption of encrypted conversations when authorized by a court order and would require at all encryption products manufactured, sold, or imported into the United States be capable of providing decryption of communications upon the court-ordered request of law enforcement, while also limiting the release of the seized communications, much like present law provides when a wire, oral or electronic intercept has been made.

The proposed amendment makes no change of Federal (or State) policy. Congress has wisely authorized the interception of communications by court order. The proposed amendment will simply assure that law enforcement may continue to do so in this age of electronic encryption.

I urge you and the Committee to support this amendment. To allow law enforcement the real and effective access to decryption of encrypted communications is absolutely essential to the continued effectiveness of investigative efforts. Let me be clear, if decryption is not provided for, Federal and State law enforcement agencies will be unable to effectively develop the crucial evidence of conspiracies and other violations of law that have been instrumental in addressing organized crime in its various forms. I trust that the importance and the value of the proposed amendment will be recognized by you and the Committee members.

Should you desire additional information from me, please do not hesitate to call me at (850) 488–8771. I ask that you share this letter with the Committee as it meets in "markup" this afternoon and whenever you consider H.R. 695.

Sincerely,

JAMES T. MOORE, *Commissioner.*

CITY OF CINCINNATI,
DIVISION OF POLICE,
September 23, 1997.

Congressman MICHAEL G. OXLEY,
Committee on Commerce, Rayburn House Office Bldg., Washington, DC.

DEAR CONGRESSMAN: I urge you to strongly consider the needs of law enforcement with respect to H.R. 695 when it comes before your committee on September 26, 1997. As it is written, H.R. 695 would permit the marketing of encryption products that would severely impair law enforcement's ability to lawfully gain access to criminal telephone conversations and electronically stored evidence.

Law enforcement recognizes that encryption is necessary for communications security and privacy. We also understand that commercial interests are at stake in marketing of these products. Adequate legislation is the key to satisfying these needs and maintain the ability of law enforcement to combat serious crime. The use of non-key recovery encryption would severely hamper our efforts.

The amended version of H.R. 695, offered by Congressman Oxley, Ohio and Congressman Manton, New York, requires manufacturers to include some form of recovery feature in encryption products sold in the United States. This would allow law enforcement the opportunity to gather criminal information when legally authorized to do so.

Your consideration in this matter is of the utmost importance to the continued effort of maintaining public safety.

Sincerely,

MICHAEL C. SNOWDEN, *Police Chief.*

CITY OF PHOENIX,
OFFICE OF THE POLICE CHIEF,
September 24, 1997.

Hon. MICHAEL G. OXLEY,
Committee on Commerce, Rayburn House Office Building, Washington, DC.

DEAR MR. OXLEY: I am aware that you are presently considering a variety of legislative proposals concerning the encryption of electronic information. While I recognize the need to encrypt communications for reasons of personal security, privacy, and safe electronic commerce, it is imperative that law enforcement be provided a feature that allows us, upon presentation of a court order, to gain timely access to plain text data through decryption. It is an undeniable fact that unrestricted use of strong encryption will cripple law enforcement's ability to use wiretaps and other measures to catch criminals and terrorists. Loss of this essential ability at a time

when international drug trafficking, white collar crime, and terrorist activities are on the rise, would be disastrous.

It should be noted that law enforcement's current judicially controlled wiretap capabilities have not resulted in misuse because adequate checks and balances prevail.

I believe that any attempt to adopt a voluntary key recovery system is unacceptable. If only one vendor of a strong encryption product opts not to participate, or if unrestricted foreign products are imported, it will take time for these products to become the products of choice for criminal activities.

Other countries have, and will continue to, develop strong encryption software that does not allow for key recovery. Little will be gained from restricting U.S. vendors from marketing competitive products to these countries. If however, any country establishes a key recovery requirement, as we should in the U.S., a ban with accompanying legal penalties should apply to the use and import of all non-compliant products.

Clearly, law enforcement must have the ability to collect and decipher evidence of criminal and terrorist activities. We solicit your support in preserving law enforcement's ability to protect the public from serious crime.

Sincerely,

DENNIS A. GARRETT, *Police Chief.*

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

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

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

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

tably detract from the security of the Department of Defense and the nation.

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

I appreciate your consideration of these views.

Sincerely,

BILL COHEN.

ADDITIONAL VIEWS

The stated intent of H.R. 695, the removal of barriers to the competitiveness of U.S. high technology exports, is a goal with which few Members of Congress, the business community, or our law enforcement organizations could disagree. As reported by the Committee on Commerce, however, H.R. 695 inadequately addresses the legitimate public safety concerns surrounding the proliferation of strong encryption technology within our own borders.

The bombings this decade alone at the Alfred P. Murrah Federal Building in Oklahoma City, Oklahoma and at New York's World Trade Center attest to the present dangers terrorist attacks pose to our citizens. The high tech world increasing presents the committed men and women who keep our nation safe with new and more daunting challenges in their fight against domestic and foreign criminals. The decisions Congress makes at the doorstep of the digital age will have serious repercussions lasting long past our own tenures in Congress and must be guided by more than economics.

New encryption technologies have the potential to provide Americans with a level of security in telecommunications and electronic commerce never before available. At the same time, however, the widespread availability of such technology could render sophisticated criminals invisible to the lawful surveillance efforts of federal, state and local law enforcement.

Congress need not provide government agencies with an increased ability to access the communications of suspected criminals to overcome the challenges posed by encryption. Congress need only ensure that the thoughtful and painstaking procedures law enforcement officials must presently abide by before commencing any surveillance operation continue to yield an ability to monitor the activities of those who threaten the safety of the American people.

In our opinion, Congress must balance the needs of American's technological entrepreneurs with its fundamental duty to ensure public safety. We believe the goal of further promoting U.S. technology exports can be achieved in a version of H.R. 695 that does not threaten the safety of the American people. Though not entirely satisfied with H.R. 695 as reported out of the Commerce Committee, we look forward to addressing the bill's deficiencies on the House floor this Congress.

EDOLPHUS TOWNS.
FRANK PALLONE, Jr.
RICK C. LAZIO.
BART STUPAK.

ADDITIONAL VIEWS OF HON. JOHN D. DINGELL

Historically, encryption was used almost exclusively by the military and intelligence communities to protect secrets of defense and national security. But in the Information Age, businesses and consumers need a way to secure valuable trade and financial information that increasingly flows through wires and over the air.

H.R. 695 attempts to accomplish these important goals by bringing export law in line with current domestic encryption policy. Unfortunately, such a change in the law does not come without a cost. While strong encryption can make interstate and foreign commerce more secure, its unrestricted use can make national security and law enforcement less so.

It is clear that widespread use of unbreakable encryption poses serious problems for law enforcement in carrying out its duty to protect the public. Even in the post-cold war era, the wars against international terrorism, drug cartels, and violations of human rights continue.

The law enforcement community advocates the use of key recovery systems on strong encryption products. Unfortunately, these system will work only if everybody uses them, including sophisticated criminals. And we know that there will continue to be a proliferation of encryption products available around the would without key recovery systems, regardless of U.S. Government law or policy.

I am not convinced that the law enforcement approach will solve the problem the authorities correctly identify. But until a better solution is proposed that both protects the public against terrorism and removes barriers to the growth of electronic commerce around the world, I strongly believe it is in the public interest to err on the side of caution.

This bill adopts the approach preferred by business and privacy advocates which, unfortunately, also contains flaws. Removing all government controls over encryption is tantamount to sending our troops to war without necessary arms or protective gear. The committee attempted to balance the important competing interests at stake, but failed to find the elusive middle ground. H.R. 695, as amended by this committee, simply adds window dressing in the form of a technology lab. This begs more questions than it answers.

The American public has no assurance that a technology lab will be effective in providing law enforcement with the tools necessary to protect them. Without possessing a key to encrypted messages, the only way to unlock the door is through brute force. A brute force attack on today's encryption products requires both enormous computing power and a good deal of time. Law enforcement authorities possess neither luxury when confronted with an imminent, real-time threat to public safety. A technology lab will not change that reality.

Some producers of encryption products have offered informally to provide the lab with technical assistance and perhaps some amount of private funding. But we have no specific commitment with regard to either offer, nor can we be sure that any such contribution would be sufficient to achieve the lab's purpose. The industry has specifically rejected the notion of providing source code for its encryption products to the lab, which is arguably the best hope for giving law enforcement a leg up on cracking these codes without a key.

I appreciate that these issues have been the subject of intense debate for more than four years of government, industry, individual citizens, and academia alike. To date, no effective solution has been found. But the difficulty of the task does not mean that we should conduct the legislative equivalent of a coin toss. The simple fact that four other committees have reported this bill in such radically different forms should be evidence enough that while this issue may be ripe, the solution certainly is not.

In my judgment, this bill is not ready for prime time. More work needs to be done. I urge all committees that have reported versions of this bill and the bipartisan leadership to continue working with industry and law enforcement to find an effective and balanced solution before this bill reaches the floor for consideration.

JOHN D. DINGELL.

○

Document No. 9