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

SECURITY AND FREEDOM THROUGH ENCRYPTION (SAFE) ACT

MAY 22, 1997.—Ordered to be printed

Mr. COBLE, from the Committee on the Judiciary, submitted the following

REPORT

together with

ADDITIONAL VIEW

[To accompany H.R. 695]

[Including cost estimate of the Congressional Budget Office]

The Committee on the Judiciary, 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

39–006

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', 'investigative or law enforcement officer', and 'judge of competent jurisdiction' 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, the District of Columbia, or any commonwealth, territory, or possession of the United States; 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. Freedom to use encryption

"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.

"§ 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 Secu-

rity 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 5 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 10 years, or fined in the amount set forth in this title, or both.".

(b) CONFORMING AMENDMENT.—The table of chapters for part I of title 18, United States Code, is amended by inserting after the item relating to chapter 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. 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 widespread use of strong encryption to encode digital communications will prevent crime, economic espionage, and information warfare. Unfortunately, our current encryption policy discourages the use of encryption. H.R. 695, the "Security And Freedom through Encryption (SAFE) Act," makes a series of changes to U.S. encryption policy which will facilitate the use of encryption.

Current policy does not restrict the domestic use, sale, or import of encryption. Section 2 of H.R. 695 generally codifies that policy by affirmatively prohibiting restrictions on the domestic use and sale of encryption. It also prohibits any mandatory key escrow system, allowing voluntary systems to develop in the marketplace, and provides criminal penalties for the knowing and willful use of encryption to avoid detection of other federal felonies.

At the same time, however, the export of strong encryption products is tightly restricted under the export control laws. Section 3 of H.R. 695 significantly relaxes those export controls. In addition, section 4 requires that the Attorney General compile statistics on instances in which these new policies may interfere with the enforcement of federal criminal laws.

BACKGROUND AND NEED FOR THE LEGISLATION

I. BACKGROUND

A. What is encryption?

Encryption is the process of encoding data or communications in a form that only the intended recipient can understand. Until fairly recently, society generally considered encryption to be the exclusive domain of national security and law enforcement agencies. However, with the advent of computers and digital electronic communications, encryption's importance to persons and companies in the private sector has increased because they want to transmit data securely. Many people feel that the Internet has not succeeded as a commercial medium as well as it might because those who want to use it do not feel the data transmitted is secure. For example, people do not want to transmit their credit card numbers when hackers may steal those numbers.

To understand the issues involved, one must understand some basic terminology. In the digital world, data are communicated in a string of ones and zeroes that computers understand, but the average person does not. An encryption scheme converts ones to zeroes and zeroes to ones according to an algorithm or mathematical formula. The intended recipient knows the formula or "key" which he uses to decode the encrypted data.

The complexity and quality of an encryption scheme determines how difficult it is to break the code and therefore how well the scheme protects the data. One factor determining the complexity of the encryption scheme is the length of the key. The length of the key is usually expressed as a number known as the "bit length." A bit is one digit in the key. A bit length of 40 is considered relatively weak, whereas a bit length of 128 is considered very strong.

However, a bit length of 40 is not 3.2 times weaker than a bit length of 128 because this is an exponential scale, not an arithmetic one. A bit length of 40 has 2^{40} possible keys, whereas a bit length of 128 has 2^{128} possible keys. To give some practical sense of the difference, one researcher estimated that a relatively inexpensive computer attempting a "brute force" effort to decode—i.e. simply trying all the mathematical possibilities—could on average decode a 40-bit scheme in a few seconds, whereas a 128-bit scheme would on average take millions of years. Although there is no assurance that this estimate is accurate, it does give a general sense of the exponential differences in complexity that flow from an increase in bit length.

B. Issues in the encryption debate

The encryption debate encompasses two main issues. The first issue is whether the domestic use and sale of encryption products should be restricted, and in particular, whether domestic users should be required to place their keys in escrow with the government or some other neutral third party, e.g. an existing computer company or an entity created solely for the purpose of holding keys. Current law does not have any such restrictions.

The second issue is whether the export of encryption products should be restricted. As discussed in more detail below, current law

regulates the export of encryption products under two statutes: (1) the Arms Export Control Act ("AECA"), 22 U.S.C. § 2751 et seq., and its accompanying International Trafficking in Arms Regulations ("ITAR"), 22 C.F.R. § 120 et seq., and (2) the Export Administration Act ("EAA"), 50 U.S.C. App. § 2401 et seq., and its accompanying Export Administration Regulations ("EAR"), 15 C.F.R. § 730 et seq. Although the EAA expired in 1994, President Clinton kept its provisions in force by invoking his powers under the International Emergency Economic Powers Act, 50 U.S.C. § 1701 et seq. Executive Order 12924 (August 19, 1994); 59 Fed. Reg. 43437 (August 23, 1994).

1. Arguments relating to the domestic use of encryption

Law enforcement and national security agencies believe that they need some form of key escrow system to maintain their ability to perform legitimate wiretaps and to read computer data seized through lawful means. They argue that widespread use of strong encryption without key escrow would end the use of wiretapping as a tool for fighting crime. For example, they argue that instances occur when law enforcement agencies learn in the course of a wiretap that someone is about to commit a serious crime. If strong encryption prevented a contemporaneous understanding of this information, the agencies would not be able to prevent the crime. Likewise, if strong encryption prevented the reading of lawfully seized computer data, it could unreasonably delay criminal investigations. They further argue that a key escrow system would have the salutary side effect of providing a backup for those users who might lose their keys. Although they contend that they only favor a voluntary key escrow system, many believe that the use of export controls as leverage to encourage the use of a key escrow system effectively amounts to making such a system mandatory.

The computer industry, the American business community, and privacy groups vehemently oppose any mandatory key escrow system. They argue that a mandatory system would unnecessarily invade the privacy of users and that the market should develop any voluntary key escrow system. They believe that law enforcement can gain access to keys through traditional means for obtaining evidence and that those with criminal intent will not use key escrow products, thus defeating the purpose of the Administration's policy. They argue that our law and tradition do not require private citizens to take positive action to assist the government in surveilling them in any other instance.

Moreover, they contend that private citizens should not be required to give access to their most precious assets to anyone else regardless of whether it is the government or a third party. In the digital age, information is often the most valuable property that a company owns. They further argue that the good that widespread use of encryption can do in preventing crime far outweighs the harm done by the relatively few instances in which the use of encryption hampers law enforcement.

2. The administration's recent initiative

Until last fall, the Administration treated encryption products as munitions for export purposes. The State Department has jurisdic-

tion over the export of munitions under AECA and ITAR, and it had, as a matter of practice, generally only allowed the export of encryption products with bit lengths of 40 or less. The State Department treated these relatively weak encryption products as non-defense products subject to the jurisdiction of the Department of Commerce under the Export Administration Act, 50 U.S.C. App. § 2401 et seq. Beyond that level, any export of encryption products required a special license.

On October 1, 1996, Vice President Gore announced the Administration's intention to develop a new policy on the export of encryption products. The Vice President's announcement stated in part:

> Under this initiative, the export of 56-bit key length encryption products will be permitted under a general license after one-time review, and contingent upon industry commitments to build and market future products that support key recovery. This policy will apply to hardware and software products. The relaxation of controls will last up to two years.
>
> * * * * * * *
>
> Exporters of 56-bit DES or equivalent encryption products would make commitments to develop and sell products that support the key recovery system that I announced in July. That vision presumes that a trusted party (in some cases internal to the user's organization) would recover the user's confidentiality key for the user or for law enforcement officials acting under proper authority. Access to keys would be provided in accordance with destination country policies and bilateral understandings. No key length limits or algorithm restrictions will apply to exported key recovery products.
>
> * * * * * * *
>
> Under the relaxation, six-month general export licenses will be issued after one-time review, contingent on commitments from exporters to explicit benchmarks and milestones for developing and incorporating key recovery features into their products and services, and for building the supporting infrastructure internationally. Initial approval will be contingent on firms providing a plan for implementing key recovery. The plan will explain in detail the steps the applicant will take to develop, produce, distribute, and/or market encryption products with key recovery features. The specific commitments will depend on the applicant's line of business.
>
> The government will renew the licenses for additional six-month periods if milestones are met. Two years from now, the export of 56-bit products that do not support key recovery will no longer be permitted. Currently exportable 40-bit mass market software products will continue to be exportable. We will continue to support financial institutions in their efforts to assure the recovery of encrypted financial information. Longer key lengths will continue to be

approved for products dedicated to the support of financial applications.

Statement of the Vice President dated October 1, 1996.

On November 15, 1996, President Clinton issued Executive Order 13026, 61 Fed. Reg. 58767 (November 19, 1996), and an accompanying Presidential Memorandum which began the implementation of the policy outlined in the October 1 statement. Among other things, the executive order and the memorandum transferred all non-military encryption products to the Commerce Control List, meaning that their licensing for export would be overseen by the Department of Commerce under the EAA. The order and memorandum also gave the Department of Justice a significant voice in such licensing decisions.

On December 30, 1996, the Department of Commerce promulgated regulations that implemented the new policy. 61 Fed. Reg. 68572 (December 30, 1996). Although the policy has only been in place for a few months, much of the computer industry, particularly software companies, have criticized it.

3. Arguments relating to export controls on encryption products

The Administration has to date opposed any lifting of export controls beyond that in its recent initiative. It argues that the controls are still effective and that our allies would dislike the negative effect on law enforcement efforts if we lifted the controls. It also argues that the lifting of the controls might not help business because other countries would impose import controls. Finally, the Administration argues that it is making efforts under its new policy to find ways to relax the controls on a case by case basis.

The computer industry and the privacy groups argue that the Administration ought to substantially relax, if not eliminate the controls. They argue that wrongdoers can easily evade them because many encryption products are available to anyone over the Internet. At least one study estimated that at least 500 products are available worldwide. They also argue that the controls are easily evaded because as a practical matter, anyone can come into the United States, buy encryption products, and take them out of the country with little risk of detection. Because the controls are so easily evaded, they further argue that the controls serve only to put American companies at a competitive disadvantage and to discourage investment in the development of better encryption products. If the situation does not change, they believe that American companies will no longer dominate this field.

In addition, they contend that the Administration's new policy is a backdoor attempt to force the domestic use of encryption with key escrow. Under the policy, a company that wants both to sell encryption products here and abroad must either make two versions of its product or sell only a product that meets the export restrictions. They also question whether the carrot and stick approach the new policy takes is a legitimate and logical use of export controls. Current encryption products of the 56-bit strength are either safe to export or they are not—a company's compliance or noncompliance with the Administration's directives regarding future products will not change that.

4. Recent litigation

Currently, at least two plaintiffs have ongoing lawsuits that challenge the Administration's policies regarding encryption. In one case, the United States District Court for the District of Columbia ruled that the government's decision to designate an encryption product as a munition, and therefore restrict its export, was not subject to judicial review. *Karn* v. *Department of State*, 925 F.Supp. 1 (D.D.C. 1996), *remanded*, 107 F.3d 923 (D.C. Cir. 1997). The Court further held that the export restriction on the product was content neutral and narrowly tailored, and therefore did not violate the First Amendment. The United States Court of Appeals for the District of Columbia Circuit recently remanded the case for further consideration in light of the Administration's new policy, and the Committee understands that the Court has not made a further decision. The plaintiff in the case, Philip Karn, testified before the Subcommittee on Courts and Intellectual Property at the March 20, 1997 hearing on H.R. 695.

In the other case, the United States District Court for the Northern District of California ruled that the export restrictions on encryption products were unconstitutional prior restraints on free speech because they did not have adequate procedural safeguards. *Bernstein* v. *Department of State*, 945 F.Supp. 1279 (N.D. Cal. 1996). The Committee understands that this case is still before the District Court for further consideration in light of the Administration's new policy.

II. NEED FOR THE LEGISLATION

A. Sections 2 and 4—domestic use of encryption

The Committee believes that sections 2 and 4 of H.R. 695, as reported by the Committee, will significantly aid the fight against crime. Both sides of the debate agree that the use of strong encryption will help users to prevent crimes before they happen. As we increasingly depend on computers to control our national infrastructure, the danger of information warfare and economic espionage also increase. The use of strong encryption diminishes that terrifying prospect.

The affirmative statements in new sections 2802 and 2803 that it is legal for persons in the United States and for United States persons abroad to use, and for persons in the United States to sell, encryption will encourage the use of encryption to fight crime. These sections only state what the Committee understands to be existing law, and therefore they should not worsen any law enforcement and national security concerns. By making these affirmative statements of positive law, the bill will prevent any reduction of the existing right to use or sell encryption domestically by administrative action, state law, or other means.

New section 2804 effectively prohibits the imposition of any mandatory key escrow system. The Committee believes that Americans should not be forced to surrender the keys to their data without proper justification any more than they should be forced to surrender the keys to their homes. The limited circumstances under which law enforcement and national security officers may obtain access to the private spaces of Americans have stood the test of

time. They exist for good reasons that are well understood by all. The advent of a new technology is not a sufficient justification for diminishing these historic protections.

At the same time, however, new section 2804 preserves existing authorities for law enforcement and national security officers to obtain keys for legitimate purposes. Just as new technology should not take away the longstanding rights of citizens against government, it also should not take away the traditional means for legitimate law enforcement and national security investigations. However, the Committee does not believe that the advance of technology warrants a system of forcing people to deposit their keys with any third party without proper justification. Thus, new section 2804 prohibits any such system.

Despite the Committee's opposition to any mandatory key escrow system, nothing in section 2804 should be construed to prevent or hinder the development of a voluntary key escrow system if the market demands it. Such a system may have many benefits so long as users are allowed to choose freely whether to join. If enough users desire it, the Committee believes that the market will develop it.

In addition to the preservation of existing law enforcement authorities to obtain keys for legitimate purposes in new section 2804, new section 2805 further aids law enforcement and national security by making it a crime to avoid detection of another federal felony through the knowing and willful use of encryption. This section gives the government another tool with which to fight the misuse of encryption.

Section 4 requires the Attorney General to compile and make available to Congress information on instances in which encryption interferes with the enforcement of the federal criminal law. This requirement will assist the Committee in determining whether to make any further changes to encryption policy. It will also foster a continuing dialogue between the Congress and the executive branch on these matters. Through all of these means, the Committee believes that it has carefully balanced the needs of law abiding citizens against those of the law enforcement and national security agencies as to the matters within its jurisdiction.

B. Section 3—export controls

Section 3 of H.R. 695 significantly relaxes existing export controls on encryption products. Because Section 3 amends the Export Administration Act of 1979, it falls within the jurisdiction of the House Committee on International Relations. The International Relations Committee has been given a secondary referral of H.R. 695 for consideration of Section 3.

For that reason, the Committee on the Judiciary did not address Section 3 during its consideration of H.R. 695. However, the Committee realizes that export controls must be addressed as part of any comprehensive national encryption policy. The Committee believes that it has carefully balanced the interests involved in the matters under its jurisdiction. It stands ready to work with the Committee on International Relations, the Administration, and all other interested parties in an effort to develop a similar, but more

comprehensive, balancing of all the interests, including those relating to export controls, as this legislation moves forward.

HEARINGS

The Committee's Subcommittee on Courts and Intellectual Property held one day of hearings on H.R. 695 on March 20, 1997. The Subcommittee received testimony from the following twelve witnesses: Hon. William Reinsch, Under Secretary, Bureau of Export Administration, Department of Commerce, Washington, D.C.; Hon. William Crowell, Deputy Director, National Security Agency, Fort Meade, Maryland; Hon. Robert Litt, Deputy Assistant Attorney General, Criminal Division, United States Department of Justice, Washington, D.C.; Mrs. Phyllis Schlafly, President, Eagle Forum, St. Louis, Missouri; Mr. Ira Rubinstein, Senior Corporate Attorney, Microsoft Corporation, on behalf of the Business Software Alliance; Ms. Roberta Katz, Senior Vice-President, General Counsel, and Secretary, Netscape Communications Corporation, Mountain View, California, on behalf of the Information Technology Association of America and the Software Publishers Association; Mr. Jonathan Seybold, Chairman of the Executive Committee and Director, Pretty Good Privacy, Inc., San Mateo, California; Mr. Tom Morehouse, President and Chief Executive Officer, SourceFile, Inc., Oakland, California; Mr. Grover Norquist, President, Americans for Tax Reform, Washington, D.C.; Mr. Philip Karn, Staff Engineer, Qualcomm, Inc., San Diego, California; Mr. Marc Rotenberg, Director, Electronic Privacy Information Center, Washington, D.C.; and Mr. Jerry Berman, Executive Director, Center for Democracy and Technology, Washington, D.C. Two organizations submitted additional material for the record.

In addition, Congressman Goodlatte introduced identical legislation, H.R. 3011, in the 104th Congress. The full Committee held one day of hearings on H.R. 3011 on September 25, 1996 (Serial No. 100). The Committee received testimony from the following eight witnesses: Hon. Bob Goodlatte, United States Representative, 6th District of Virginia; Hon. Jamie Gorelick, Deputy Attorney General, United States Department of Justice, Washington, D.C.; Hon. William Crowell, Deputy Director, National Security Agency, Fort Meade, Maryland; Hon. William Reinsch, Under Secretary, Bureau of Export Administration, Department of Commerce, Washington, D.C.; Ms. Melinda Brown, Vice-President and General Counsel, Lotus Development Corporation, Cambridge, Massachusetts, on behalf of the Business Software Alliance; Ms. Roberta Katz, Senior Vice-President, General Counsel, and Secretary, Netscape Communications Corporation, Mountain View, California, on behalf of the Information Technology Association of America and the Software Publishers Association; Ms. Patricia Ripley, Managing Director, Bear Stearns & Company, Inc., New York, New York; and Dr. Charles Deneka, Senior Vice-President and Chief Technology Officer, Corning, Inc., Corning, New York, on behalf of the National Association of Manufacturers. Two organizations submitted additional material for the record.

COMMITTEE CONSIDERATION

On April 30, 1997, the Subcommittee on Courts and Intellectual Property met in open session and ordered reported the bill H.R. 695 without amendment, by a voice vote, a quorum being present. On May 14, 1997, the Committee met in open session and ordered reported favorably the bill H.R. 695 with a single amendment in the nature of a substitute, by a voice vote, a quorum being present.

VOTE OF THE COMMITTEE

During their consideration of H.R. 695, the Committee and the Subcommittee took no roll call votes.

COMMITTEE OVERSIGHT FINDINGS

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

COMMITTEE ON GOVERNMENT REFORM AND OVERSIGHT FINDINGS

No findings or recommendations of the Committee on Government Reform and Oversight were received as referred to in clause 2(l)(3)(D) of rule XI of the Rules of the House of Representatives.

NEW BUDGET AUTHORITY AND TAX EXPENDITURES

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

CONGRESSIONAL BUDGET OFFICE COST ESTIMATE

In compliance with clause 2(l)(3)(C) of rule XI of the Rules of the House of Representatives, the Committee sets forth, with respect to the bill, H.R. 695, the following estimate and comparison prepared by the Director of the Congressional Budget Office under section 403 of the Congressional Budget Act of 1974:

U.S. CONGRESS,
CONGRESSIONAL BUDGET OFFICE,
Washington, DC, May 21, 1997.

Hon. HENRY J. HYDE,
Chairman, Committee on the Judiciary,
House of Representatives, Washington, DC.

DEAR MR. CHAIRMAN: The Congressional Budget Office has prepared the enclosed cost estimate for H.R. 695, the Security and Freedom Through Encryption (SAFE) Act.

If you wish further details on this estimate, we will be pleased to provide them. The CBO staff contacts are Rachel Forward (for

federal costs); Stephanie Weiner (for revenues); and Leo Lex (for the state and local impact).

Sincerely,

JAMES L. BLUM
(For 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 technologies to any third party. The bill also would prevent the Bureau of Export Administration (BXA) in the Department of Commerce from restricting the export of most nonmilitary encryption products. H.R. 695 would establish criminal penalties and fines for the use of encryption technologies to conceal incriminating information relating to a felony from law enforcement officials. Finally, the bill would require the Attorney General to maintain data on the instances in which encryption impedes or obstructs the ability of the Department of Justice (DOJ) to enforce the criminal laws.

Assuming appropriation of the necessary amounts, CBO estimates that enacting this bill would result in additional discretionary spending of between $1 million and $3 million over the 1998–2002 period of BXA and DOJ. Spending by BXA and DOJ for activities required by H.R. 695 would total between $5 million and $7 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 beginning in fiscal year 1998 through the imposition of criminal fines and the resulting spending from the Crime Victims Fund. Therefore, pay-as-you-go procedures would apply. CBO estimates, however, that the amounts of additional direct spending or receipts would not be significant.

H.R. 695 contains no private-sector mandates as defined in the Unfunded Mandates Reform Act of 1995 (UMRA). The bill would prohibit states from requiring persons to make encryption keys available to another person or entity. This prohibition would be an intergovernmental mandate as defined in UMRA. However, states would bear no costs as a result of the mandate because none currently require the registration or availability of such keys.

Estimated cost to the Federal Government: 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.

According to the DOJ, maintaining data on the instances in which encryption impedes or obstructs the ability of the Department of Justice to enforce the criminal laws could cost $1 million or more per year. The cost of maintaining the data is difficult to ascertain because DOJ believes that if H.R. 695 were enacted such instances would be numerous. But the agency is uncertain as to how much it would cost to track such classified information nationwide. For the purposes of this estimate, CBO projects that maintaining the data would cost DOJ between $500,000 and $1 million a year, assuming appropriation of the necessary amounts.

CBO estimates that the collections of criminal fines for the use of encryption technologies to conceal incriminating information relating to a felony from law enforcement officials would not be significant.

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

Pay-as-you-go considerations: Section 25 of the Balanced Budget and Deficit Control Act of 1985 sets up pay-as-you-go procedures for legislation affecting direct spending or receipts through 1998. Enacting H.R. 695 would affect direct spending and receipts through the imposition of criminal fines for encrypting incriminating information related to a felony. 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 amount as the amount of fines collected with a one-year lag, the additional direct spending would also be negligible.

Estimated impact on State, local, and tribal governments: H.R. 695 would prohibit states from requiring persons to make encryption keys available to another person or entity. This prohibition would be an intergovernmental mandate as defined in UMRA. However, states would bear no costs as the result of the mandate because none currently require the registration or availability of such keys.

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

Estimate prepared by: Federal Costs: Rachel Forward—Revenues: Stephanie Weiner—Impact on State, Local, and Tribal Governments: Leo Lex.

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

CONSTITUTIONAL AUTHORITY STATEMENT

Pursuant to rule XI, clause 2(l)(4) of the Rules of the House of Representatives, the Committee finds the authority for this legislation in Article I, section 8 of the Constitution.

SECTION-BY-SECTION ANALYSIS

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 122 in Title 18 of the United States Code. This chapter 122 would include new sections 2801–05.

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. § 2510 et seq. During the Committee markup, Mr. Delahunt offered an amendment making technical changes to these definitions to conform them more closely with the existing definitions. The Delahunt amendment passed on a voice vote.

New section 2802 affirmatively states that it is legal for any person in the United States, or any United States person in a foreign country, to use any form of encryption regardless of the algorithm, key length, or technique used in the encryption. New section 2803 affirmatively 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. Some business groups have expressed concern that new sections 2802 and 2803 might be construed to override their lawful policies for employee use of their computer systems. The Committee does not intend for these sections to be so read. The Committee intends that these sections 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 systems, nor as limiting the employer's otherwise lawful means for remedying violations of those policies.

Thus, even though employees cannot be prosecuted for an offense of unlawful encryption under Section 2802, employees may be prosecuted for failing to return business property, unlawful appropriation, or conversion. Consider, for example, the case in which an employer's information management policy calls for company-wide deployment of key recovery encryption, and a given employee refuses to comply, encrypting instead without key recovery using some other system. In that instance, the employer remains within his rights, under state statutory or common law, to sue to obtain the needed key to recover the business property—plans, designs, texts, databases, and the like—contained in the computer or computers under the employee's control.

New section 2804 specifically prohibits requiring any person in lawful possession of an encryption key to turn that key over to another person. This section effectively prevents any form of mandatory key escrow system. As introduced, this section provided an exception for law enforcement personnel acting under any law in effect on the date of enactment. At the Committee markup, Mr. McCollum offered an amendment that expands the exception to include members of the intelligence community as defined in section 3 of the National Security Act of 1947 (50 U.S.C. § 401a). The McCollum amendment passed by a voice vote.

Finally, new section 2805 makes it a crime to use encryption unlawfully in furtherance of some other crime. This new crime is punishable by a sentence of 5 years for the first offense and 10 years for a subsequent offense. The Delahunt amendment that made technical changes to the definitions also changed the language of this section. The Delahunt amendment clarified two points relating to this new crime: (1) it applies only to the use of encryption to avoid detection of some other federal felony, and (2) it applies only when the encryption is knowingly and willfully used to avoid detection. In other words, this crime cannot occur without the commission of some other federal felony, and the use of encryption must be a deliberate attempt to avoid detection of that felony. It may not be unknowing or accidental. As noted above, the Delahunt amendment passed on a voice vote.

Subsection 2(b) of H.R. 695 provides for a conforming amendment to the table of chapters in Title 18.

Section 3. Exports of Encryption. Subsection 3(a) of H.R. 695 amends the Export Administration Act by creating a new subsection (g) to 50 U.S.C. App. §2416. New subsection (g)(1) would place all encryption products, except those specifically designed or modified for military use, under the jurisdiction of the Secretary of Commerce. New subsection (g)(2) allows encryption software that is generally available or in the public domain, like mass-market software products, to be exported freely. New subsection (g)(3) requires the Secretary to allow other encryption software to be exported unless there is substantial evidence that it will be put to military or terrorist uses or that it will be reexported without U.S. authorization.

New subsection (g)(4) requires the Secretary to allow the export of hardware with encryption capabilities when the Commerce Department finds that it is commercially available from foreign suppliers without effective restrictions. New subsection (g)(5) provides definitions.

The Committee would like to clarify that with the ever increasing incorporation of computer-like intelligence (including hardware and software) into consumer products for the protection of privacy, information security, and intellectual property interests, it intends this legislation to cover all devices—whether traditional "computing" devices or "convergent" consumer products—that incorporate encryption. Further, the applications covered by this legislation include video, audio, and data communications systems. Hardware and software containing encryption, such as encoders, decoders, and network terminals, which are essential to protect the video signal, are therefore included under section 3(a) of this Act. Video, audio, and data communications systems containing encryption and decryption capability are used by cable, satellite, and wireless delivery systems.

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. Effect on Law Enforcement Activities. Section 4 was not part of the bill as introduced. An amendment offered by Mr. Hutchinson added this language to the bill. Subsection 4(a) requires the Attorney General to compile information on instances in which encryption has interfered with, impeded, or obstructed the ability of the Justice Department to enforce federal criminal law and to maintain that information in classified form. The Committee intends that information compiled by the Attorney General pursuant to this section also include instances in which encryption has prevented crimes from occurring, especially in protecting national infrastructures and preventing economic espionage (although not limited to those areas). Subsection 4(b) requires that the Attorney General shall make the information compiled under subsection 4(a), including an unclassified summary, available to Members of Congress upon request. The Hutchinson amendment passed on a voice vote.

AGENCY VIEWS

U.S. DEPARTMENT OF JUSTICE,
OFFICE OF LEGISLATIVE AFFAIRS,
Washington, DC, April 30, 1997.

Hon. HOWARD COBLE,
Chairman, Subcommittee on Courts and Intellectual Property, Committee on the Judiciary, House of Representatives, Washington, DC.

DEAR MR. CHAIRMAN: Your Subcommittee will soon begin mark-up of H.R. 695, the "Security and Freedom Through Encryption (SAFE) Act." Although the Department of Justice supports H.R. 695's overall goal of promoting the wide dissemination of strong encryption, we believe that the bill would severely compromise law enforcement's ability to protect the American people from the threats posed by terrorists, organized crime, child pornographers, drug cartels, financial predators, hostile foreign intelligence agents, and other criminals. In addition, the bill would greatly impair the government's ability to prosecute those crimes when they do occur. We urge the Subcommittee to reject H.R. 695 in its present form.

There is widespread agreement that strong encryption is essential to the success of the emerging Global Information Infrastructure (GII). Communications and data must be protected—both in transit and in storage—if the GII is to be used for personal communications, financial transactions, medical care, the development of new intellectual property, and myriad other applications. Having recognized the importance of encryption, we must ensure that its application is consistent with the larger goals of society. One approach, that taken by H.R. 695 advocates the proliferation of unbreakable encryption that would not only protect commerce and privacy, but also unintentionally protect criminals. A better approach, advocated by the Administration, encourages the use of data recovery products that fully protect commerce and privacy, but without sacrificing public safety and national security.

Viewed in this light, the proposed legislation poses two major problems for federal, state, and local law enforcement. First, it would effectively eliminate all export controls on strong encryption,

thereby undermining public safety and national security by encouraging the proliferation of unbreakable encryption. Second, the bill discourages formation of a key management infrastructure that addresses the needs of public safety, economic security and privacy.

The elimination of export controls would adversely affect national security and foreign policy interests and severely impair many law enforcement efforts at the federal, state and local level. We have heard, of course, the oft-repeated argument that the "genie is already out of the bottle"—that strong encryption is already widely available overseas and over the Internet and that attempts to limit its spread are futile, and serve only to handicap U.S. manufacturers seeking to sell their encryption products overseas. In fact, this is not the case.

Although strong encryption products can be found overseas, these products are not ubiquitous, in part because the export of strong encryption is controlled by both the U.S. and other countries. It is worth noting in this regard that export of encryption over the Internet, like any other means of export, is restricted under U.S. law. Although it is difficult to prevent completely encryption products from being sent abroad over the Internet, we believe that the legal restrictions will limit the use of the Internet as a means of evading export controls.

In addition, the quality of encryption products offered abroad varies greatly, with some encryption products not providing the levels of protection advertised. Finally, the vast majority of businesses with a serious need for strong encryption are not likely to rely on encryption downloaded from the Internet from untested sources, but will prefer instead to deal with known and reliable suppliers. For these reasons, export controls continue to serve a critical function.

A few other factors are important to consider regarding export controls. First, our allies strongly concur that unrestricted export of encryption would severely hamper law enforcement objectives. It would be a terrible irony if this government—which prides itself on its leadership in fighting international crime—were to enact a law that would jeopardize public safety and weaken law enforcement agencies worldwide.

Second, critics of export controls have mistakenly assumed that the lifting of export controls would result in unrestricted access to markets abroad by U.S. companies. But this assumption ignores the likely reaction of foreign governments to the elimination of U.S. export controls. To date, most other countries have not needed to restrict imports or domestic use of encryption, largely because export controls in the U.S.—the world leader in computer technology—and other countries have made such restrictions unnecessary. But given other countries' legitimate concerns about the potential worldwide proliferation of unbreakable encryption products, we believe that many of those countries would respond to any lifting of U.S. export controls by imposing import controls, or by restricting use of strong encryption by their citizens.

France, Russia and Israel, for example, have already established domestic restrictions on the import, manufacture, sale and use of encryption products. In addition, a number of European Union countries are moving towards the adoption of a key-recovery-based

key management infrastructure similar to that proposed by the Administration. In the long run, then, U.S. companies might not be any better off if U.S. export controls were lifted, but the would have undermined our leadership role in fighting international crime and damaged our own national security interests in the meantime.

We also oppose H.R. 695 because it would impede or prevent the development of a key management infrastructure. The bill could be read as prohibiting the United States government from using appropriate incentives to support a key management infrastructure and key recovery. Without such an infrastructure supporting key recovery, federal law enforcement investigations will become far more difficult. The problems that enactment of H.R. 695 would pose for state and local law enforcement, which lack access to supercomputers, are even greater.

In law enforcement, quick action can save lives, reduce crime and apprehend criminals. Criminals, therefore, rely on techniques that help them slow or prevent law enforcement officers from detecting and solving crimes and catching offenders. The passage of H.R. 695 could unintentionally add a powerful new technique—unbreakable encryption—to the collection of methods that criminals use to thwart law enforcement and prey upon the residents of the United States. It is difficult enough to fight crime without making criminals' tasks any easier.

The Subcommittee should approve a bill that encourages the development of a key management infrastructure and key recovery system coupled with responsible export controls. We look forward to working with you in developing an approach to encryption that meets the dual goals of maintaining law enforcement's ability to fight crime and protecting the right to privacy within the burgeoning global information infrastructure. We are hopeful that by working together we can create a mutually acceptable national encryption policy. The Office of Management and Budget has advised that there is no objection from the standpoint of the Administration's program to the presentation of this report.

Sincerely,

ANDREW FOIS,
Assistant Attorney General.

CHANGES IN EXISTING LAW MADE BY THE BILL, AS REPORTED

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

TITLE 18, UNITED STATES CODE

* * * * * * *

PART I—CRIMES

CHAPTER 125—ENCRYPTED WIRE AND ELECTRONIC INFORMATION

§2801. Definitions

As used in this chapter—

(1) the terms "person", "State", "wire communication", "electronic communication", "investigative or law enforcement officer", and "judge of competent jurisdiction" 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, the District of Columbia, or any commonwealth, territory, or possession of the United States; 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. Freedom to use encryption

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.

§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 5 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 10 years, or fined in the amount set forth in this title, or both.

* * * * * * *

SECTION 17 OF THE EXPORT ADMINISTRATION ACT OF 1979

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 nec-

essary 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.

ADDITIONAL VIEWS OF HON. BOB GOODLATTE

H.R. 695, the Security And Freedom through Encryption (SAFE) Act of 1997, accomplishes three critical goals: preventing economic crime, promoting electronic commerce, and protecting the personal privacy of all law-abiding Americans. I am pleased that both the Courts and Intellectual Property Subcommittee and the full Judiciary Committee have approved this bipartisan legislation by voice vote. I would also like to thank the lead cosponsor of the SAFE Act, Rep. Zoe Lofgren (D–CA), for her leadership. support, and dedication to this important issue.

The Administration's encryption policies are at odds with its stated goals. For example, the Administration has stated in testimony before both the House and Senate that it supports the widespread use of strong encryption. However, the Administration continues to enforce antiquated Cold War export restrictions that prevent the widespread use of strong encryption.

The Department of Justice has been particularly hostile to H.R. 695, even going so far as publicly stating that the bill would be devastating to international law enforcement. As an example, just hours prior to Subcommittee markup of H.R. 695 on April 30, 1997, the Department of Justice circulated a letter to Judiciary Committee members opposing the legislation. This letter contained a series of allegations which deserve a response.

> DOJ Claim: The bill "discourages formation of a key management infrastructure".
>
> Response: The SAFE Act takes no position on the development of a key management infrastructure.

The term "key management infrastructure" refers to a system, yet to be fully developed, that would allow Internet users to know with whom they are communicating, to verify document signatures, and to identify whether documents are tampered with or altered in transmission. Such a system could partly operate through "Certificate Authorities", or commercial entities that would certify, like digital notary publics, that certain public keys are in fact the keys of particular individuals or corporations.

Driven by user needs, the on-line world is developing such systems of assurance without government intervention. The security and effectiveness of these systems will be tested by the market. Consequently, it is impossible to know at this point which systems will succeed and which will fail—the intensely competitive global marketplace will decide that question. Government bureaucracy and regulation is neither necessary nor desirable.

Perhaps the greatest impediment to the development of a widespread global key management infrastructure to date has been the Administration's restrictive export policies. By preventing American companies from exporting strong encryption, this Administra-

tion has perpetuated a sense of uncertainty in the global market that has discouraged these companies from developing commercial infrastructures. Contrary to the Administration's claim, therefore, H.R. 695 would actually promote development of Certificate Authorities and key management infrastructures in the best way possible, by removing unwanted, unworkable, and unwise government bureaucracy and regulation.

A recent report issued by nine of the world's top cryptographers, entitled "The Risks of Key Recovery, Key Escrow, and Trusted Third Party Encryption", offers further evidence that various key escrow, key recovery. and key management systems that have been proposed by the Administration are neither feasible nor advisable. As stated In this report:

> Government key recovery proposals call for one of the most ambitious and far-reaching deployments of the information age. The field of cryptography has no experience in deploying secure systems of this scope and complexity. * * * Attempts to force the widespread adoption of key recovery encryption through export controls, import or domestic use regulations, or international standards should be considered in light of these factors. The public must carefully consider the costs and benefits of embracing government-access key recovery before imposing the new security risks and spending the huge investment required—potentially many billions of dollars, in direct and indirect costs—to deploy a global key recovery infrastructure.

The Administration has stated publicly that "only industry can build a robust and scalable key management infrastructure". This report shows quite clearly that proposals to establish global key management systems, including incentives to use such systems, are at best premature. As former British Prime Minister Margaret Thatcher aptly put it, "Governments * * * are themselves 'blind forces' blundering about in the dark, and obstructing the operations of markets rather than improving them."

> DOJ Claim: Strong encryption is not widely available overseas, in part because of U.S. export controls.
>
> Response: German, Dutch, Swedish, British, Russian and other foreign manufacturers have created strong and reliable encryption products that are available internationally and on the Internet.

As evidence of this, the following excerpt is from a recent New York Times article discussing the success of a German company, Brokat Informationsysteme, which produces a 128-bit encryption program:

> Far from hindering the spread of powerful encryption programs * * * American policy has created a bonanza for alert entrepreneurs outside the United States. When America Online wanted to offer on-line banking and shopping services in Europe, it turned to Brokat for the software that encodes transactions and protects them from hackers and on-line bandits. When Netscape Communications and Microsoft wanted to sell Internet software to

> Germany's biggest banks, they had to team up with Brokat to deliver the security guarantees that the banks demanded. * * * Besides America Online, Brokat's customers include more than 30 big banking and financial institutions around Europe.

Perhaps a more vivid example of the folly of the Administration's export restrictions is the recent announcement that Sun Microsystems, one of the leading U.S. computer companies, will be entering into a partnership with Elvis+, a Russian encryption manufacturer, to distribute strong encryption worldwide. Since the U.S. has no import or domestic controls on the use of non-key escrow encryption, Sun can import the Russian product and distribute it domestically, while the Russian company distributes the same product overseas. Therefore, U.S. companies will now be able to securely communicate with their overseas offices and subsidiaries without violating the export control laws.

The Sun announcement demonstrates three critical facts that reveal the absurdity of arguments the Administration uses to defend its current policies: (1) consumers are demanding strong encryption products to protect their digital communications; (2) strong encryption products are already available from foreign manufacturers, and reputable U.S. firms are willing to stake their corporate reputations on the quality of those products; and (3) the current export control scheme is taking jobs and revenue away from our economy.

Additionally, many individuals and small businesses rely on the Pretty Good Privacy encryption program, which is available on the Internet worldwide. PGP is equivalent to 128-bit encryption, and has been tested again and again. It is based on a public algorithm, so every hacker, graduate student, and computer scientist in the world can try to break it. None have succeeded.

> DOJ Claim: If the U.S. were to relax its current export controls on strong encryption, foreign governments would respond by creating import controls on U.S. products and thus those markets would not open to U.S. companies.
>
> Response: The United States should not set its export policies on the basis of actions that other countries might take.

The U.S. government should not stand in the way of our industry's ability to compete in the global marketplace—in fact, it should use any resources available to help American companies succeed in global markets. When foreign governments raise import barriers to keep out U.S. products, they do so to allow their own industries to dominate the marketplace. We should not allow ourselves to be fooled into believing otherwise.

> DOJ Claim: H.R. 695 would "adversely affect national security and foreign policy interests and severely impair many law enforcement efforts at the federal, state, and local level."
>
> Response: Strong encryption prevents crime. Consider the findings of the National Research Council on the use of strong encryption:

> If cryptography can protect the trade secrets and proprietary information of businesses and thereby reduce economic espionage (which it can). it also supports in a most important manner the job of law enforcement. If cryptography can help protect nationally critical information systems and networks against unauthorized penetration (which it can), it also supports the national security of the United States.

When criminals talk to other criminals, they will always be able to use strong encryption, with no mechanism for law enforcement access, to protect their communications. The Administration's policy will not prevent this, since it is not proposing direct domestic or import controls on strong encryption, and cannot prevent foreign companies from developing and distributing such products. However, when these criminals communicate with legitimate organizations, such as banks, law enforcement will always be able to obtain evidence from such organizations via court order or grand jury subpoena. Therefore, allowing law-abiding people to use strong encryption to protect themselves, and allowing U.S. companies to fully compete in the global marketplace, will not prevent law enforcement from pursuing and stopping criminals.

It is truly ironic that law enforcement agencies would oppose legislation that prevents crime. Unfortunately, it seems that the Administration does not want to empower our citizens and our industries to protect themselves in the Information Age. Just as deadbolt locks and alarm systems help people protect their houses against intruders, thereby assisting law enforcement in preventing crime, strong encryption allows people to protect their digital communications and computer systems against criminal hackers and computer thieves.

The SAFE Act prevents crime, promotes commerce, and protects privacy. Additionally, it allows the free market to design its own standards and solutions for the development of global commerce, free from unwanted and unworkable government regulation. This bipartisan legislation ensures that all law-abiding Americans will be able to communicate and conduct business securely in the Information Age.

BOB GOODLATTE.

ADDITIONAL MINORITY VIEWS

We offer these additional views not to foment dissent but to encourage dialogue with the Administration on the issues related to encryption. We would like to work with federal law enforcement and national security agencies to address their concerns.

We sympathize with the difficulties faced by investigative and security agencies in combating crime, terrorism, and espionage. We believe it is quite legitimate for the Administration to be concerned about the uncertain impact that strong and ubiquitous encryption products may have on law enforcement and national security agencies. We realize that it may ultimately become impossible for government agencies to decipher intercepted or retrieved data and communications that have, by encryption, been transformed into a seemingly unintelligible form.

We recognize the days of cracking strong codes are nearly gone. Unbreakable codes (256-bit key algorithms can generate more possible solutions than there are particles in the known universe) are already widely known. Private security experts and sophisticated hackers have already realized this and are beginning to develop ways of attacking the vulnerable points before and after the information is encrypted (i.e., on the sender's hard drive or at a "good-guy" recipient such as a bank). We suspect that law enforcement and national security experts within the government are acquiring similar capabilities. But these alternative (and more subtle) approaches are not reflected in the Administration's current public policy toward encryption.

The Administration's current encryption policy, a policy that runs back at least to the Bush Administration, creates more problems than it resolves. The policy is a combination of encryption export controls and a key escrow system by which the key to the code encrypting the information is to be held by a third party (so it may be made available to the government).

We need to be honest about this situation. We don't expect most narcotics traffickers, terrorists, or criminals to respect export restrictions on encryption when they don't respect our underlying drugs or weapons laws. And we don't generally expect anyone who employs encryption in furtherance of a crime to readily give their keys to some third party so they may be made available to the government.

The Administration maintains that there is a commercial need for key recovery. While that may be true to some extent, there appears to be little or no demand for the all-encompassing system they want to mandate. Experts have uniformly concluded the government's proposed system is either excessively costly and complex or insecure. In part, this is true because the government seeks access to real-time communications and data transmissions, rather than the ability to recover stored data.

The Administration insists it doesn't want domestic restrictions on encryption. We are concerned, however, that the Administration policy does have this effect. Development of software programs, including those utilizing encryption, occurs at an amazingly rapid pace, so it is not feasible for computer software and hardware companies to develop separate products for export and for domestic use. As a result, as a practical matter, only products that are exportable, with weaker encryption or with government-approved key recovery-escrow, can be marketed at present.

We fear that current encryption policy, encouraging as it does weaker encryption, makes every American more vulnerable to illicit or surreptitious access to our computer files, our phone conversations, and personal information, and thus exposes our citizens to hackers, terrorists, and thieves. It is ironic that what is trumpeted as an aid to law enforcement may instead compromise individual and corporate security.

What we have here is not only a combination of export controls and a key recovery system that does not work, we have a system that compromises the competitiveness and security of this nation's software and hardware industry, as well as our privacy rights. As conceded by Administration witnesses, the proposed key recovery system can succeed only as long as there is no non-conforming encryption software readily available in the market. But there is already an abundance of such software, some of it freeware, that is readily available over the Internet.

The proposed key recovery system can not work unless the United States persuades every other nation to adopt key recovery. We can safely say we are unlikely to obtain the agreement of Libya, Iran, Iraq, or North Korea. In addition, the efforts to date of David Aaron, U.S. Ambassador to the Organization for Economic Cooperation and Development (OECD), to obtain a consensus in support of key recovery resulted instead in a consensus opposing it.

The Administration's policy has therefore been a strong market incentive:

(a) for non-participants (in the Administration's key escrow program) to make non-standard, secure encryption available, and

(b) for U.S. companies to set up abroad in "encryption havens" so they may legally market strong, secure encryption products to customers who decline to make their "international key" available to diverse governments around the world.

There are already U.S. companies establishing ties with foreign companies in Japan, Russia, and elsewhere.

Nor is this policy without its cost. It is estimated that, if the U.S. persists in its current policy through the year 2000, we shall lose 200,000 jobs and $60 billion each year. This is what it will cost this nation to lose the cryptography lead we enjoy and the competitive expertise necessary to maintain our market position.

Unfortunately, our discussions to date with law enforcement and intelligence agencies have not admitted of the possibility of any further relaxation of export restrictions as part of the broader process essential to resolving this complex question. Nor has the Administration offered to consider alternatives to its key escrow or key recovery system.

H.R. 695 need not be the end of the process but the beginning of a real dialogue. This is what we would like to happen. We continue to remain hopeful that the Administration will acknowledge the shortcomings of its current policy and sincerely hope that this will happen soon lest more serious damage be done to our industry, to our security and to our privacy.

JOHN CONYERS, Jr.
RICK BOUCHER.
ZOE LOFGREN.
MAXINE WATERS.
WILLIAM DELAHUNT.
MARTIN T. MEEHAN.

○

Document No. 5