AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

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

SECURITY AND FREEDOM THROUGH ENCRYPTION (SAFE) ACT

APRIL 27, 1999.—Ordered to be printed

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

R E P O R T

together with

ADDITIONAL VIEWS

[To accompany H.R. 850]

[Including cost estimate of the Congressional Budget Office]

The Committee on the Judiciary, to whom was referred the bill (H.R. 850) to amend title 18, United States Code, to affirm the rights of United States persons to use and sell encryption and to relax export controls on encryption, having considered the same, report favorably thereon without amendment and recommend that the bill do pass.

CONTENTS

	Page
Purpose and Summary	2
Background and Need for Legislation	2
I. Background	2
A. What is Encryption?	2
B. Issues in the Encryption Debate	3
1. Arguments Relating to the Domestic Use of Encryption	3
2. The White House Initiative	4
3. Arguments Relating to Export Controls on Encryption Products	6
4. Recent Litigation	6
II. Need for Legislation	7
A. Sections 2 and 4—Domestic Use of Encryption	7
B. Section 3—Export Controls	8
Hearings	9
Committee Consideration	9
Vote of the Committee	9
Committee Oversight Findings	9

69–006

Committee on Government Reform Findings 9
New Budget Authority and Tax Expenditures 9
Congressional Budget Office Cost Estimate 9
Constitutional Authority Statement 12
Section-by-Section Analysis 12
Agency Views 14
Changes in Existing Law Made by the Bill, as Reported 23
Additional Views 30

PURPOSE AND SUMMARY

The widespread use of strong encryption to encode digital communications will prevent crime, economic espionage, and information warfare. Unfortunately, this country's current encryption policy discourages the use of encryption. H.R. 850, 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. 850 generally codifies that policy by affirmatively prohibiting restrictions on the domestic use and sale of encryption. It also prohibits the government from imposing a 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. 850 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 have argued that widespread use of strong encryption without key escrow would end the use of wiretapping as a tool for fighting crime. For example, they have argued 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 read-

ing of lawfully seized computer data, it could unreasonably delay criminal investigations. They further have argued 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 White House Initiative

Until 1996, encryption products were treated as munitions for export purposes. The State Department has jurisdiction 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 (emphasis added).

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).

On September 16, 1998, the Administration announced an update to its encryption policy. Among its provisions, the new policy states U.S. firms can export any level of encryption to their foreign subsidiaries, except for certain terrorist states. The policy will also permit export of encryption products over 56-bit to 46 countries without a license to certain industries including banks, insurance companies, hospitals, HMO's, medical labs, civilian government agencies, non military health organizations, and online merchants (for example, communications between merchants and customers, like buying a book or clothes from an online catalog). A Tech Center will be created whose stated purpose is to help law enforcement

understand technology. Under the updated policy, exports to countries other than the 46 specific countries require a license, although the application has a presumption of approval; 56-bit encryption can be exported without restriction after a one-time review. The policy fails to codify the current right of all Americans to use any type of encryption they choose. This omission opens the door for the Administration to change its domestic encryption policy in the future without congressional authorization. For key recovery products, the policy directs proponents will need a license to export to foreign commercial firms but not for export to telecommunications companies or Internet service providers. The new Administration policy will be reviewed after one year.

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 initiatives. 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 estimate contends that over 650 strong and reliable 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 the 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

At least two plaintiffs have challenged 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 there-

fore restrict its export, was not subject to judicial review. *Karn* v. *Department of State,* 925 F.Supp. 1 (D.D.C. 1996), *remanded,* 1997 U.S. App. Lexis 3123 (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 District of Columbia Circuit Court of Appeals remanded the case for further consideration in light of the Administration's new policy.

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). Upon further review, the Court concluded that the regulation of encryption products is not prohibited by law and that the First Amendment does not remove encryption technology entirely from all government regulation. However, the Court ruled in favor of the plaintiff as it applied to his publishing of scientific papers, algorithms, or computer programs. *Bernstein* v. *Department of State,* 974 F.Supp. 1288 (N.D. Cal. 1997).

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. 850, 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 ob-

tain 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; however, it also states that the mere use of encryption alone cannot be the basis for establishing probable cause with respect to a search warrant or in a criminal investigation.

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. 850 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. 850 for consideration of Section 3.

For that reason, the Committee on the Judiciary did not address Section 3 during its consideration of H.R. 850. 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

On Thursday, March 4, 1999, the Subcommittee on Courts and Intellectual Property held a hearing on H.R. 850, the "Security and Freedom Through Encryption (SAFE) Act." The following individuals testified at the March 4th hearing: William Reinsch, Undersecretary of Commerce for Export Administration, United States Department of Commerce; Ronald D. Lee, Associate Deputy Attorney General, United States Department of Justice; Barbara McNamara, Deputy Director, National Security Administration; Tom Parenty, Data and Communications Security, Sybase, Incorporated; Craig McLaughlin, Chief Technology Officer, Privada, Incorporated; Grover Norquist, President, Americans for Tax Reform; Professor Dorothy E. Denning, Georgetown University; Alan B. Davidson, Staff Counsel, Center for Democracy and Technology; Ed Gillespie, Executive Director, Americans for Computer Privacy; and Dave McCurdy, President, Electronic Industries Alliance.

COMMITTEE CONSIDERATION

On March 11, 1999, the Subcommittee on Courts and Intellectual Property met in open session and ordered reported the bill H.R. 850 without amendment, by a voice vote, a quorum being present. On March 24, 1999, the Committee met in open session and ordered reported favorably the bill H.R. 850 without amendment, by a voice vote, a quorum being present.

VOTE OF THE COMMITTEE

During their consideration of H.R. 850, the Committee and the Subcommittee took no rollcall votes.

COMMITTEE OVERSIGHT FINDINGS

In compliance with clause 3(c)(1) 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 3(c)(4) of rule XIII of the Rules of the House of Representatives.

NEW BUDGET AUTHORITY AND TAX EXPENDITURES

Clause 3(c)(2) of House rule XIII is inapplicable because this legislation does not provide new budgetary authority or increased tax expenditures.

CONGRESSIONAL BUDGET OFFICE COST ESTIMATE

In compliance with clause 3(c)(3) of rule XIII of the Rules of the House of Representatives, the Committee sets forth, with respect to the bill, H.R. 850, the following estimate and comparison prepared

by the Director of the Congressional Budget Office under section 402 of the Congressional Budget Act of 1974:

U.S. CONGRESS,
CONGRESSIONAL BUDGET OFFICE,
Washington, DC, April 21, 1999.

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

If you wish further details on this estimate, we will be pleased to provide them. The CBO staff contacts are Mark Grabowicz (for costs of the Justice Department) and Mark Hadley (for costs of the Commerce Department), Hester Grippando (for revenues), and Leo Lex (for the state and local impact).

Sincerely,

DAN L. CRIPPEN, *Director.*

Enclosure.

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

Summary

H.R. 850 would allow individuals in the United States to use and sell any form of encryption and would prohibit states or the federal government from requiring individuals to relinquish the key to encryption 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. 850 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 implementing H.R. 850 would result in additional discretionary spending, by DOJ, of $3 million to $5 million over the 2000–2004 period. (The department's spending for activities related to encryption exports is negligible under current law.) Enacting H.R. 850 also would affect direct spending and receipts, beginning in fiscal year 2000, 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 and receipts would not be significant.

H.R. 850 contains no new private-sector mandates as defined in the Unfunded Mandates Reform Act (UMRA). The bill would preempt state laws that require the use of encryption products or services in a number of circumstances. These preemptions would be intergovernmental mandates as defined in UMRA, but the cost to states would be small and would not exceed the threshold estab-

lished in UMRA ($50 million in 1996, adjusted annually for inflation).

Estimated Cost to the Federal Government

The expense of compiling and maintaining data on the instances in which encryption impedes or obstructs the ability of the department to enforce the criminal laws is difficult to ascertain because the number of such instances is unknown—but DOJ believes that if H.R. 850 were enacted they would be numerous. CBO estimates that such efforts would cost DOJ between $500,000 and $1 million a year, assuming appropriation of the necessary amounts. These costs would fall within budget function 750 (administration of justice).

Under current policy, BXA would likely spend about $500,000 a year reviewing exports of encryption products, pursuant to a November 1996 executive order and memorandum that authorized BXA to control the export of all nonmilitary encryption products. If H.R. 850 were enacted, BXA would still be required to review requests to export most computer hardware and software with encryption capabilities. Thus, enacting H.R. 850 would not significantly affect BXA's spending.

CBO estimates that the collections from criminal fines established by the bill—for the use of encryption technologies to conceal incriminating information relating to a felony—would not be significant.

Pay-As-You-Go Considerations

The Balanced Budget and Emergency Deficit Control Act sets up pay-as-you-go procedures for legislation affecting direct spending or receipts. H.R. 850 would affect direct spending and receipts by imposing criminal fines 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 additional 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 would also be negligible.

Estimated Impact on State, Local, and Tribal Governments

H.R. 850 would preempt state laws that require encryption keys to be built into computer systems or to be registered with an outside entity or retained by the owner. The bill would also preempt state laws that require the use of encryption for authenticating documents or for ensuring their confidentiality. Both preemptions would be mandates as defined in UMRA. The preemptions of state law would apply to all entities in the state, but they would also prevent the states themselves from using certain types of encryption technology. The direct impact on state budgets would depend upon the degree to which they are using and will use such technology. Most states have not implemented electronic systems that use encryption, so the impact of the bill on current operations would be small.

CBO has no basis for predicting the degree to which states would use encryption technology in the future in the absence of this legislation. Encryption that is prohibited by the bill includes the scrambling of electronically stored or transmitted information in order to preserve confidentiality, integrity, or authenticity. Thus, the bill may preclude states from using digital signatures to send or receive legal documents electronically. Digital signatures consist of a stream of electronically coded text that uses the body of the document itself, along with unique identifying information about the sender, to authenticate the document and its sender. They are generated through the use of mathematical algorithms, and they can be validated by using electronic keys.

The use of digital signatures would provide options to states and other entities that wish to send legal documents electronically, rather than as hard copies. Resulting reductions in paperwork and distribution costs could lead to cost savings. However, CBO estimates that any lost savings or other costs of the mandates to states would not exceed the threshold established in UMRA ($50 million in 1996, adjusted annually for inflation).

Estimated Impact on the Private Sector

This bill would impose no new private-sector mandates as defined in UMRA.

Estimate Prepared By:

Federal Costs: Mark Grabowicz for DOJ and Mark Hadley for BXA.

Revenues: Hester Grippando.

Impact on State, Local, and Tribal Governments: Leo Lex.

Estimate Approved By:

Robert A. Sunshine, Deputy Assistant Director for Budget Analysis.

[See Additional Views, Statement of Representative Bob Goodlatte disagreeing with the CBO letter.]

CONSTITUTIONAL AUTHORITY STATEMENT

Pursuant to clause 3(d)(1) of rule XIII 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. Title

This section states that the title of the bill is the Security and Freedom Through Encryption (SAFE) Act.

Section 2. Domestic use and sale of encryption; prohibition on mandatory key escrow; use of encryption in furtherance of a federal felony

This section creates a new chapter in title 18 of the U.S. Code regarding the use and sale of encryption within the United States, the prohibition of a mandatory key escrow system, and the unlawful use of encryption in furtherance of a criminal act.

New section 2801 contains a series of definitions relating to encryption. New section 2802 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.

New section 2803 states that it is legal for any person in the United States to sell any type of encryption product in interstate commerce. New section 2804 prohibits the federal government or a state from requiring or conditioning approval on a requirement that encryption products be built with a third-party access feature (also known as "key escrow" or "key recovery") or that persons with control over decryption keys provide access to someone other than the key owner. This section also prohibits the federal government or a state from establishing conditions, ties, or links between encryption products and the issuance of certificate authorities or digital signatures. Exceptions to this section exist for law enforcement or intelligence officers seeking access to encrypted information and where the federal government or a state wishes to use key escrow/key recovery encryption for its own systems.

New section 2805 makes it a crime to use encryption unlawfully in furtherance of some other crime. This new crime is punishable with a sentence of 5 years for a first offense and 10 years for a second or subsequent offense. To trigger the provisions of this section, a person must be convicted of or plead guilty to a federal felony in which the person knowingly and willfully used encryption to conceal that felony for the purpose of avoiding detection by law enforcement. This section also states that the use of encryption cannot, by itself, be the basis for establishing probable cause with respect to a criminal offense or a search warrant.

Section 3. Exports of encryption

This section makes a series of changes to the export of encryption products. Subsection (a) amends the Export Administration Act of 1979 by creating a new subsection (g) regarding encryption products and products containing encryption or encryption capabilities.

New subsection (g)(1) places all encryption products, except those specifically designed or modified for military use, under the jurisdiction of the Secretary of Commerce. New subsection (g)(2) states that after a one-time, 15-day technical review by the Secretary, no export license may be required for generally available encryption software and hardware products, generally available products containing encryption, generally available products with encryption capabilities, technical assistance and data used to install or maintain generally available encryption products, products containing encryption, and products with encryption capabilities, and encryption products not used for confidentiality purposes.

New subsection (g)(3) states that after a one-time, 15-day technical review by the Secretary, the Secretary shall allow the export of custom-designed encryption products and custom-designed products with encryption capabilities if those products are permitted for use by banks or if comparable products are commercially available outside the U.S. An exception to this subsection exists if there is substantial evidence that these products will be diverted or modified for military or terrorist use or reexported without authorization.

New subsection (g)(4) creates a series of definitions relating to encryption products, products containing encryption, products containing encryption capabilities, and the export of such products for this subsection.

Subsection (b) states that encryption products that do not require an export license as of the date of enactment of this Act shall not require an export license on or after that date.

Subsection (c) states that nothing in this Act shall limit the authority of the President to prohibit the export of encryption products to terrorist nations or nations that have been determined to repeatedly support acts of international terrorism, or to impose an embargo on exports to and imports from a specific country. This subsection also allows the Secretary of Commerce to prohibit the export of specific encryption products to specific individuals or organizations in specific foreign countries, if the Secretary determines that there is substantial evidence that such products will be used for military or terrorist purposes.

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

Section 4. Study on the effect of encryption on law enforcement activities

This section requires the Attorney General to compile information on the instances in which encryption has interfered with, impeded, or obstructed the ability of the Justice Department to enforce the criminal laws of the United States.

AGENCY VIEWS

DEPARTMENT OF JUSTICE,
FEDERAL BUREAU OF INVESTIGATION,
Washington, DC, March 3, 1999.

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

DEAR MR. CHAIRMAN: Enclosed please find copies of resolutions and letters from various law enforcement associations and groups which set forth their positions concerning encryption. Even though these letters were prepared during the last Congress, the positions set forth in them remain unchanged. You and the Members of the Subcommittee may find this information helpful as you begin consideration of H.R. 850, the "Security and Freedom Through Encryption (SAFE) Act," a bill to relax existing export controls on encryption.

Encryption is becoming a fact of everyday life in today's information age and a natural consequence of technology. Encryption is extremely beneficial when used legitimately to protect sensitive electronically stored information and the privacy of communications. But the use of strong, unbreakable encryption by hostile governments and by criminals and terrorists for illegal purposes poses a significant and unacceptable threat to our national security capabilities.

As you know, export controls on encryption products exist primarily to protect national security and foreign policy interests. On occasion, U.S. law enforcement is provided with valuable criminal-related information obtained through our Nation's intelligence gathering efforts. Law enforcement believes that such intelligence gathering capabilities derived, in part, from export controls on encryption should be preserved.

The law enforcement community continues to support the adoption of a balanced encryption policy. Such a balanced policy must satisfy the needs of commerce and communications privacy, the national security needs of the Intelligence Community as well as the public safety needs of law enforcement. We look forward to working with the Subcommittee and the Congress in an effort to develop a balanced encryption policy that effectively addresses all parties' concerns regarding this most important privacy, commerce, national security and public safety issue.

Sincerely yours,

JOHN E. COLLINGWOOD,
Assistant Director, Office of Public and Congressional Affairs.

INTERNATIONAL ASSOCIATION OF CHIEFS OF POLICE

ENCRYPTION

Submitted by: Legislative Committee

L006.a96

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

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

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

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

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

Whereas, government representatives have been working with industry to encourage the voluntary development, sale, and use of

key-escrow encryption in its pursuit of a balanced encryption policy; now, therefore, be it

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

NATIONAL SHERIFFS' ASSOCIATION

RESOLUTION

DIGITAL TELECOMMUNICATIONS ENCRYPTION

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

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

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

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

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

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

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

Adopted at a meeting of the Membership on this 19th day of June, 1996 in Portland, Oregon

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 for private sector use; and

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

Whereas, the law enforcement community is extremely concerned about the serious threat posed by the use of 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.

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

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

DEAR MR. CHAIRMAN: The Major Cities Chiefs is a professional association of police executives representing the largest jurisdictions in the United States. The association provides a forum for

urban police chiefs, sheriffs and other law enforcement chief executives to discuss common problems associated with protecting cities with populations exceeding 500,000 people.

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

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

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

Sincerely yours,

MATT RODRIGUEZ,
Chairman.

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

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

We fully recognize that encryption is critical to communications security and privacy, and that substantial commercial interests are at stake. Perhaps in recognition of these facts, all the bills being considered allow market forces to shape the development of

encryption products. We, too, place substantial reliance on market forces to promote electronic security and privacy, but believe that we cannot rely solely on market forces to protect the public safety and national security. Obviously, the government cannot abdicate its solemn responsibility to protect public safety and national security.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

In sum, while encryption is certainly a commercial interest of great importance to this Nation, it is not solely a commercial or business issue. Those of us charged with the protection of public safety and national security, believe that the misuse of encryption technology will become a matter of life and death in many instances. That is why we urge you to adopt a balanced approach that accomplishes the goals mentioned above. Only this approach will allow police departments, attorneys general, district attorneys, sheriffs, and federal authorities to continue to use their most effective investigative techniques, with court approval, to fight crime and espionage and prevent terrorism.

Sincerely yours,

JANET RENO,
Attorney General.

LOUIS FREEH,
Director, Federal Bureau of Investigation.

THOMAS A. CONSTANTINE,
Director, Drug Enforcement Administration.

RAYMOND W. KELLY,
Undersecretary for Enforcement, U.S. Department of Treasury.

JOHN W. MAGAW,
Director, Bureau of Alcohol, Tobacco and Firearms.

BARRY MCCAFFREY,
Director, Office of National Drug Control Policy.

LEWIS C. MERLETTI,
Director, United States Secret Service.

GEORGE J. WEISE,
Commissioner, United States Customs Service.

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

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

Any encryption legislation that does not ensure that law enforcement can gain timely access to the plaintext of encrypted conversations and information by established legal procedures will cause grave harm to public safety. The risk cannot be left to the uncertainty of market forces or commercial interests as the current legislative proposals would require. Without adequate safeguards, the unbridled use of powerful encryption soon will deprive law enforcement of two or its most effective tools, court authorized electronic surveillance and the search and seizure of information stored in computers. This will substantially tip the balance in the fight against crime towards society's most dangerous criminals as the information age develops.

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

Sincerely yours,

DARRELL L. SANDERS,
President, International Association of Chiefs of Police.

JAMES E. DOYLE,
President, National Association of Attorneys General.

FRED SCORALIC,
President, National Sheriffs' Association.

WILLIAM L. MURPHY,
President, National District Attorneys Association.

DEPARTMENT OF DEFENSE,
DEPUTY SECRETARY OF DEFENSE,
Washington, DC, March 24, 1999.

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

DEAR MR. CHAIRMAN: On March 11, 1999 the House Judiciary Subcommittee on Courts and Intellectual Property passed the Goodlatte Bill (H.R. 850, "Security and Freedom Through Encryption (SAFE) Act"). I am writing to let you know that the Defense Department has deep reservations about this legislation. We believe that the bill, in its current form, threatens our ability to undertake critical national security activities.

Let me say at the outset that the Department strongly supports encryption. Indeed, we believe it is essential since we increasingly operate critical command and control functions over commercial systems. Encryption is critical for us to maintain confidentiality of our communications. But at the same time, we and the law enforcement community have an obligation to protect American security interests through the timely delivery of intelligence to decision-makers. The passage of legislation that immediately decontrols the export of strong encryption will result in the loss or delay of essential intelligence reporting because it may take too long to decrypt the information—if indeed we can decrypt it at all. Our nation cannot have an effective decision-making process, a strong fighting force, or a responsive law enforcement community unless the required intelligence information is available in time to make a difference. H.R. 850 threatens our ability to do just that.

The Department of Defense worked closely with other elements of the Administration, with Congress and with the software industry last year to craft encryption export regulations that provided maximum opportunity to American industry while still preserving essential restraints critical for national security. H.R. 850 threatens that balance and would seriously weaken our national security. I must ask for your help in bringing the full picture to bear on your deliberations as you review this legislation.

Sincerely,

JOHN J. HAMRE.

CHANGES IN EXISTING LAW MADE BY THE BILL, AS REPORTED

In compliance with clause 3(e) of rule XIII of the Rules of the House of Representatives, changes in existing law made by the bill, as reported, are shown as follows (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

Chap.		Sec.
1.	**General provisions**	**1**
*	* * * * * *	
125.	***Encrypted wire and electronic information***	***2801***
*	* * * * * *	

CHAPTER 125—ENCRYPTED WIRE AND ELECTRONIC INFORMATION

2801. Definitions.
2802. Freedom to use encryption.
2803. Freedom to sell encryption.
2804. Prohibition on mandatory key escrow.
2805. Unlawful use of encryption in furtherance of a criminal act.

§ 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 term "decrypt" means to retransform or unscramble encrypted data, including communications, to its readable form;

(3) the terms "encrypt", "encrypted", and "encryption" mean 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;

(4) 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

(5) the term "key recovery information" means information that would enable obtaining the key of a user of encryption;

(6) the term "plaintext access capability" means any method or mechanism which would provide information in readable form prior to its being encrypted or after it has been decrypted;

(7) 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) GENERAL PROHIBITION.—Neither the Federal Government nor a State may require that, or condition any approval on a requirement that, a key, access to a key, key recovery information, or any other plaintext access capability be—

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

(2) given to any other person, including a Federal Government agency or an entity in the private sector that may be certified or approved by the Federal Government or a State to receive it; or

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

(b) PROHIBITION ON LINKAGE OF DIFFERENT USES OF ENCRYPTION.—Neither the Federal Government nor a State may—

(1) require the use of encryption products, standards, or services used for confidentiality purposes, as a condition of the use of such products, standards, or services for authenticity or integrity purposes; or

(2) require the use of encryption products, standards, or services used for authenticity or integrity purposes, as a condition of the use of such products, standards, or services for confidentiality purposes.

(c) 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

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

(1) in the case of a first offense under this section, shall be imprisoned for not more than 5 years, or fined 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) USE OF ENCRYPTION NOT A BASIS FOR PROBABLE CAUSE.—The use of encryption by any person shall not be the sole basis for establishing probable cause with respect to a criminal offense or a search warrant.

* * * * * * *

SECTION 17 OF THE EXPORT ADMINISTRATION ACT

EFFECT ON OTHER ACTS

SEC. 17. (a) * * *

* * * * * * *

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

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

(2) ITEMS NOT REQUIRING LICENSES.—After a one-time, 15-day technical review by the Secretary, no export license may be required, except pursuant to the Trading With the Enemy Act or the International Emergency Economic Powers Act (but only to the extent that the authority of such Act is not exercised to extend controls imposed under this Act), for the export or reexport of—

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

(i) that is generally available;

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

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

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

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

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

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

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

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

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

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

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

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

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

(3) COMPUTER HARDWARE OR SOFTWARE OR COMPUTING DEVICES WITH ENCRYPTION CAPABILITIES.—After a one-time, 15-day technical review by the Secretary, the Secretary shall authorize the export or reexport of computer hardware or software or computing devices with encryption capabilities for nonmilitary end uses in any country—

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

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

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

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

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

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

(A)(i) the term "encryption" means the scrambling of wire communications, electronic communications, or electroni-

cally 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;

(ii) the terms "wire communication" and "electronic communication" have the meanings given those terms in section 2510 of title 18, United States Code;

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

(i) computer hardware or computer software that is—

(I) distributed through the Internet;

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

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

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

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

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

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

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

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

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

(C) 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;

(D) the term "computer hardware" includes, but is not limited to, computer systems, equipment, application-specific assemblies, smart cards, modules, integrated circuits, and printed circuit board assemblies;

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

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

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

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

ADDITIONAL VIEWS

H.R. 850, the Security and Freedom Through Encryption (SAFE) Act of 1999, 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 without amendment 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, and to note that the bill currently has 250 cosponsors, including a majority of the leadership on both sides of the aisle.

The Congressional Budget Office (CBO)'s April 21, 1999 cost estimate, submitted as a part of this Committee Report, contains a number of inaccuracies that deserve correction. In the section entitled "Estimated Impact on State, Local, and Tribal Governments," the CBO letter states that H.R. 850 "would also preempt state laws that require the use of encryption for authenticating documents or for ensuring their confidentiality." This statement is false. While the bill would preempt state laws (none of which currently exist) requiring the use of encryption for authentication or integrity as a condition of the use of encryption for confidentiality (and vice versa), H.R. 850 does not preempt state laws that require the use of encryption for authentication or the use of encryption for confidentiality. In other words, the bill would only preempt a linkage of these two uses. In fact, one of the chief purposes of this legislation is to encourage the use of encryption, not to hinder the use of encryption.

The CBO letter also incorrectly states that H.R. 850 "would also prevent the states themselves from using certain types of encryption technology." Again, the purpose of this legislation is to encourage the use of encryption, not to hinder the use of encryption. H.R. 850 only prohibits the federal government or a state from requiring that only recoverable encryption products be used in communications between private persons or between private persons and federal government or state entities. The bill does not prohibit the federal government or a state from using any type of encryption product, including a recoverable encryption product, on its own networks or systems, provided that such product is interoperable with a non-recoverable encryption product. This is true whether the federal government or state retains its own encryption keys, or uses other public or private entities to retain its encryption keys.

An additional error in the CBO letter is the statement that "Encryption that is prohibited by the bill includes the scrambling of electronically stored or transmitted information in order to preserve confidentiality, integrity, or authenticity." Encryption is the

scrambling of electronically stored or transmitted information in order to preserve confidentiality, integrity, or authenticity. Again, the bill only prohibits the federal government or a state from linking the use of encryption for confidentiality to the use of encryption for authenticity or integrity. H.R. 850 does not prohibit encryption—in fact, the purpose of the bill is to affirm the rights of U.S. persons to use and sell encryption and to relax export controls on encryption. With this statement, however, CBO is essentially arguing that the bill achieves the exact opposite of that which it was intended to achieve, which is false.

Finally, the CBO letter asserts that H.R. 850 "may preclude states from using digital signatures to send or receive legal documents electronically." To the contrary, the bill has no effect whatsoever on state electronic signature laws, except in cases in which states require the use of recoverable encryption products as a condition of giving legal recognition to electronic signatures. However, no such cases currently exist. Again, the bill simply prohibits the federal government or a state from linking the use of encryption to the use of electronic signatures or certificate authorities, not from requiring the use of encryption, electronic signatures, or certificate authorities themselves (provided that the federal government or state doesn't only require the use of recoverable encryption).

In the 105th Congress, similar legislation (H.R. 695) was reported by the Judiciary Committee, International Relations Committee, Commerce Committee, and National Security Committee (since renamed the Armed Services Committee). CBO letters were included in each of those reports, and none of those letters alleged that the legislation would prevent states from using certain types of encryption technology.

As H.R. 850 will next be considered in the 106th Congress by the International Relations Committee, there will be at least one more CBO letter regarding this bill. I look foward to working with CBO to correct the incorrect statements from its April 21 letter as H.R. 850 moves forward through the legislative process.

BOB GOODLATTE.

ADDITIONAL COMMENTS OF CONGRESSWOMAN ZOE LOFGREN

Following the Subcommittee Hearing I forwarded the following correspondence to Associate Deputy Attorney General Ron Lee with the enclosed attachment:

CONGRESS OF THE UNITED STATES,
HOUSE OF REPRESENTATIVES,
Washington, DC, April 22, 1999.

Hon. RON LEE,
Associate Deputy Attorney General,
Department of Justice, Washington, DC.

DEAR MR. LEE: During your testimony on March 4, 1999, you testified that there were "many technologies that aren't, strictly speaking, key recovery that do promote the interest of law enforcement as well as other government interests." I therefore asked you to tell me "specifically" what these "many technologies" were.

When you said, "very well," and that you would supply the requested information, our Subcommittee Chairman Howard Coble further reinforced my request when he instructed, "Give that to us in detail if you will, Mr. Lee."

But more than a month later, I don't know what these many technologies are and I have no detail at all from you. I have, however, received a letter from the Office of Legislative Affairs but that was not responsive at all.

The letter I've received (and I've attached a copy for your convenience) speaks of "active discussions" that "might help" address the problem, and what "a number of companies have suggested to [the Department of Justice]" and what are characterized as "three possible solutions."

This tardy submission by someone on your behalf is totally inadequate. Either you got it wrong at the hearing or, for some reason I can't fathom, you are withholding the very information you promised to supply.

I therefore respectfully request that you clarify which it is, either that you misspoke, or supply the information you originally promised to supply.

Sincerely,

ZOE LOFGREN,
Congresswoman.

U.S. DEPARTMENT OF JUSTICE,
OFFICE OF LEGISLATIVE AFFAIRS,
Washington, DC, April 14, 1999.

Hon. ZOE LOFGREN,
House of Representatives,
Washington, DC.

DEAR CONGRESSWOMAN LOFGREN: During Associate Deputy Attorney General Ron Lee's March 4, 1999 testimony before the Subcommittee on Courts and Intellectual Property of the Committee on the Judiciary, you asked him to write to you to identify those encryption technologies in addition to key recovery that promote the interests of law enforcement.

First, I would like to thank you for your continuing interest in this topic. You will recall that you exchanged letters on this matter with former Principal Associate Deputy Attorney General Robert S. Litt just last summer and fall. In his letter to you of September 24, 1998, Mr. Litt indicated that what law enforcement needs is, quite simply, access to the plaintext of encrypted data and communications when it has lawfu1 authority to obtain that plaintext. He also indicated that law enforcement was not seeking a one-hundred percent solution, but workable solutions that support the continued ability of law enforcement to conduct judicially authorized searches for data and interceptions of communications.

Critics of law enforcement openly insist that its demands are unattainable. However, there is nothing unattainable about industry's developing products and services that protect not only the security of encrypted data and communications but also the security and safety of the persons using those products and the public at large. It is important to remember that the goal of providing law enforcement with access to plaintext is the safety of the public.

We recognize, of course, that industry is responsible for designing and deploying information technologies, including encryption products, and that it must do so in a competitive marketplace. Both industry and government have learned that there is a market demand for products allowing access to plaintext (e.g., businesses that need to ensure the availability of data). In addition, creating a technological environment that directly, even if inadvertently, supports criminal activity by enabling criminals to act with impunity is not good for the public, industry, or the marketplace. While we are asking that industry use its creative genius to create smart solutions, those solutions will, in the long run, promote both public safety and commerce.

In this regard, industry has engaged in active discussions with law enforcement about technical solutions that might help address law enforcement's concerns. For example, a number of companies suggested to us that for some network-based encryption products there may be points in the network where plaintext exists, or where encryption can be disabled by a system administrator in response to a court order. Other products, such as corporate encryption systems, by their very nature, tend to be operated by corporate computer or network administrators, who can otherwise provide law enforcement with access to plaintext when such access is lawfully authorized. Still other products provide each individual user with the option to activate "recovery" for stored data, so that

if the user loses his key, he need not also lose his data (such "recovery-capable" products tend to use key recovery). Each of these types of products helps to meet the needs of law enforcement. And these are just three possible solutions out of a panoply that are being or may be developed by industry.

You may recall that the Administration updated its encryption export control policy in 1998, taking into account the benefits of such products for public safety worldwide. For example, "recoverable" products are approved for export to foreign commercial firms in over 40 countries. A number of companies thereafter cited this update as an excellent example of how industry and government can work together to find workable solutions.

Of course, the needs of public safety are just one of the many interests to be considered in the encryption debate. The Department of Justice supports the use of strong encryption for legitimate purposes, such as the protection of privacy, proprietary and financial information, and intellectual property, as well as combating fraud and securing electronic commerce. Based on our discussions with industry, we are hopeful that it will develop more solutions that meet these needs and also protect the safety of the public in general.

I look forward to continuing to work with you in this important area.

Sincerely,

DENNIS K. BURKE,
Acting Assistant Attorney General.

○