106TH CONGRESS
1st Session

HOUSE OF REPRESENTATIVES

REPT. 106–117
Part 4

PROTECTION OF NATIONAL SECURITY AND PUBLIC SAFETY ACT

REPORT

OF THE

COMMITTEE ON ARMED SERVICES
HOUSE OF REPRESENTATIVES

ON

H.R. 850

together with

ADDITIONAL AND SUPPLEMENTAL VIEWS

[Including cost estimate of the Congressional Budget Office]

JULY 23, 1999.—Committed to the Committee of the Whole House on the State of the Union and ordered to be printed

---

U.S. GOVERNMENT PRINTING OFFICE
58-132 WASHINGTON : 1999

CONTENTS

(III)

106TH CONGRESS } HOUSE OF REPRESENTATIVES { REPT. 106–117
1st Session } { Part 4

PROTECTION OF NATIONAL SECURITY AND PUBLIC SAFETY ACT

JULY 23, 1999.—Ordered to be printed

Mr. SPENCE, from the Committee on Armed Services, submitted the following

REPORT

together with

ADDITIONAL AND SUPPLEMENTAL VIEWS

[To accompany H.R. 850]

[Including cost estimate of the Congressional Budget Office]

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

The amendments are 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 "Protection of National Security and Public Safety Act".

SEC. 2. EXPORTS OF ENCRYPTION.

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

(b) AUTHORITY TO DENY EXPORT FOR NATIONAL SECURITY REASONS.—Notwithstanding any provision of this Act, the President may deny the export of any encryption product on the basis that its export is contrary to the national security interests of the United States.

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

SEC. 3. LICENSE EXCEPTION FOR CERTAIN ENCRYPTION PRODUCTS.

Encryption products with encryption strength equal to or less than the level identified in section 5 shall be eligible for export under a license exception if—

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

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

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

(4) the exporter, at the time of submission of the product for technical review, provides the names and addresses of its distribution chain partners.

SEC. 4. ONE-TIME PRODUCT REVIEW.

The President shall specify the information that must be submitted for the 1-time review referred to in section 3.

SEC. 5. ELIGIBILITY LEVELS.

(a) INITIAL ELIGIBILITY LEVEL.—Not later than 180 days after the date of the enactment of this Act, the President shall notify the Congress of the maximum level of encryption strength that may be exported from the United States under license exception pursuant to section 3 without harm to the national security interests of the United States. Such level shall not become effective until 30 days after such notification.

(b) PERIODIC REVIEW OF ELIGIBILITY LEVEL.—The President shall, at the end of each successive 180-day period after the notice provided to the Congress under subsection (a), notify the Congress of the maximum level of encryption strength, which may not be lower than that in effect under this section during that 180-day period, that may be exported from the United States under a license exception pursuant to section 3 without harm to the national security interests of the United States. Such level shall not become effective until 30 days after such notification.

SEC. 6. ENCRYPTION LICENSES REQUIRED.

(a) UNITED STATES PRODUCTS EXCEEDING CERTAIN BIT LENGTH.—An export license is required for the export of any encryption product designed or manufactured within the United States with an encryption strength exceeding the maximum level eligible for a license exception under section 3.

(b) REQUIREMENTS FOR EXPORT LICENSE APPLICATION.—To apply for an export license, the applicant shall submit—

(1) the product for technical review;

(2) a certification identifying—

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

(B) the expected end user of the product;

(3) in instances where the export is to a distribution chain partner—

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

(B) the name and address of the distribution chain partner; and

(4) any other information required by the President.

(c) POST-EXPORT REPORTING.—

(1) UNAUTHORIZED USE.—Any exporter of encryption products that are designed or manufactured within the United States shall submit a report to the Secretary at any time the exporter has reason to believe that any such product exported pursuant to this section is being diverted to a use or user not approved at the time of export.

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

(A) the particular product sold;

(B) the name and address of the end user of the product; and

(C) the intended use of the product sold.

SEC. 7. WAIVER AUTHORITY.

(a) IN GENERAL.—The President may by Executive order waive the applicability of any provision of section 3 to a person or entity if the President determines that the waiver is necessary to protect the national security interests of the United States. The President shall, not later than 15 days after making such determination, submit a report to the committees referred to in subsection (c) that includes

the factual basis upon which such determination was made. The report may be in classified format.

(b) WAIVERS FOR CERTAIN CLASSES OF END USERS.—The President may by Executive order waive the licensing requirements of section 6 for specific classes of end users identified as being eligible for receipt of encryption commodities and software under license exception in section 740.17 of title 15, Code of Federal Regulations, as in effect on July 17, 1999. The President shall, not later than 15 days after issuing such a waiver, submit a report to the committees referred to in subsection (c) that includes the factual basis upon which such waiver was made. The report may be in classified format.

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

SEC. 8. ENCRYPTION INDUSTRY AND INFORMATION SECURITY BOARD.

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

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

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

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

(C) The Secretary of Defense, or his or her designee.

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

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

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

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

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

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

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

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

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

(c) MEETINGS.—The Board shall meet at such times and in such places as the Secretary may prescribe, but not less frequently than every four months.

(d) FINDINGS AND RECOMMENDATIONS.—The chair of the Board shall convey the findings and recommendations of the Board to the President and to the Congress within 30 days after each meeting of the Board. The recommendations of the Board are not binding upon the President.

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

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

SEC. 9. MARKET SHARE SURVEY.

The Secretary shall, at least once every 6 months, conduct a market share survey of foreign markets for encryption products. The Secretary shall publish the results of the survey in the Federal Register. The publication shall include an assessment of the market share of each foreign encryption product in each market surveyed and a description of the general characteristics of each encryption product.

SEC. 10. DEFINITIONS.

In this Act:

(1) ENCRYPTION.—The term "encryption" means the transformation or scrambling of data, for the purpose of protecting such data, from plaintext to an unreadable or incomprehensible format, regardless of the techniques used for such transformation or scrambling and regardless of the medium in which such data occur or can be found.

(2) EXPORT AND EXPORTER.—The term "export" includes reexport, the term "exporter" includes "reexporter".

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

Amend the title so as to read:

A bill to protect national security and public safety through the balanced use of export controls on encryption products.

PURPOSE AND BACKGROUND

H.R. 850 is similar to a bill (H.R. 695) with the same name and chief sponsor introduced in the 105th Congress. It would decontrol the export of encryption software products, and computers that contain encryption software, considered to be "generally available."

The committee recognizes that the impetus for the bill stems from the explosive growth of the Internet and the rise in electronic commerce in recent years, which has led to increased concerns over information security. A growing number of individuals and businesses now have access to the Internet and the capability to transmit volumes of personal and proprietary data from one user to another nearly instantaneously. As technology advances, the risk that the secure transmission of this information may be compromised by computer "hackers" is increasing. This risk has resulted in calls for greater encryption capabilities.

Encryption is a means of scrambling or encoding electronic data so that its contents are protected from unauthorized interception or disclosure. Many software application programs already feature encryption capabilities to afford users a degree of privacy and security when conducting electronic transactions. For example, Netscape Communications Corporation's World Wide Web browser can transmit information in a secure, encrypted mode that allows individuals to order products and services by credit card over the internet with a reasonable expectation that any personal information transmitted will be protected.

The domestic use of encryption products is presently unrestricted, since their use by law-abiding citizens and companies can increase public confidence in the security of electronic transactions. However, in the hands of terrorists or criminals, the capability to scramble communications or encode information may hinder efforts to thwart planned terrorist acts or apprehend international drug smugglers. Therefore, the export of encryption capabilities is controlled for important national security and foreign policy reasons.

In particular, the committee notes that the U.S. military has made information warfare a key element of U.S. military strategy. It is a tenet of this element of U.S. strategy that the United States must be able to protect its own communications from interception while exploiting the weaknesses in the information systems and communications of potential adversaries. Much of the U.S. military's battlefield advantage relies on information dominance and the ability to decipher the communications of the enemy. Capabilities that make it more difficult for the United States to detect the plans and activities of hostile military forces could significantly degrade the technological advantage presently held by U.S. combat forces.

The Institute for National Strategic Studies at the National Defense University has identified seven areas of information warfare that could play decisive roles in combat, including electronic warfare, cyber warfare, command and control warfare, intelligence-based warfare, and so-called "hacker" warfare. The Institute's 1996

Strategic Assessment study noted the growing importance of information warfare and the desirability for U.S. exploitation of a potential adversary's vulnerabilities. The study declared that "if the United States could override an enemy's military computers, it might achieve an advantage comparable to neutralizing the enemy's command apparatus." In addition, it noted the value of attacking an adversary's commercial computer systems, i.e., banking, power, telecommunications, and safety systems. The ability to "wreak havoc" on these systems, the study noted, "would be a powerful new instrument of power." However, as technology advances, the proliferation of increasingly sophisticated and difficult to decipher encryption capabilities overseas may make it more difficult for the United States to maintain its military superiority and achieve tactical battlefield advantages.

The capabilities and security of encryption products generally depend on the length of the encryption algorithm or electronic "key" required to decrypt the data, as measured by the number of data "bits" in the key. Generally speaking, the longer the key (or number of key bits) the more secure the encryption program and the more difficult it is to "break the code." Until January 1997, U.S. policy allowed the unrestricted export of encryption software with keys up to 40 bits in length. As a result of growing concerns over the ability to protect the integrity and contents of personal and proprietary data, and in response to industry demands to market more capable encryption software overseas, export controls on U.S.-origin encryption products were relaxed in 1996 and again in 1998. This has led to concerns that U.S. export control policy is weighted more heavily toward privacy and economic concerns rather than national security considerations.

Because of their national security implications, the United States has traditionally considered encryption products to be sensitive "munitions" items and their export has been controlled by the State Department. However, in October 1996, the Clinton Administration decided to transfer jurisdiction over the export of commercial encryption products from the State Department to the Commerce Department, which is responsible for export controls on "dual use" items with military and civilian application. In addition, the Administration agreed to allow the export of encryption products with keys of up to 56 bits in length, beginning in January 1997, provided that the exporting companies develop a "key recovery" plan over the next two years that would allow access to the decryption keys by government law-enforcement agents or intelligence officials, if necessary, in order to decode scrambled information. The Administration's key recovery plan was criticized by industry as unworkable and a disincentive for foreign customers to purchase American encryption products. However, U.S. companies appeared to be complying with the key recovery requirements necessary to obtain U.S. government export approval, as the number of export licenses granted for encryption software increased.

In announcing the liberalized export control policy, Vice President Gore stated that it would "support the growth of electronic commerce, increase the security of the global information (sic.), and sustain the economic competitiveness of U.S. encryption product manufacturers * * *." However, an Administration talking points

paper on the decision noted that "this export liberalization poses risks to public safety and national security. The Administration is willing to tolerate that risk, for a limited period, in order to accelerate the development of a global key management infrastructure." In addition, in a letter to Congress in November 1996, President Clinton acknowledged that "the export of encryption products transferred to Department of Commerce control could harm national security and foreign policy interests of the United States even where comparable products are or appear to be available from foreign sources."

The purported availability of comparable encryption products from foreign sources remains a major argument used by industry to support further liberalization of export controls. According to a recently-released study conducted by George Washington University's Cyberspace Policy Institute (CPI), more than 800 encryption products are now available overseas in 35 countries—a 22 percent increase in the past year and a half. However, the national security community has argued that many of these products do not perform as advertised or are not effectively utilized. In addition, as the CPI study notes, only 20 percent of these products contain "strong" encryption. In testimony before the committee on July 1, 1999, Deputy Secretary of Defense John Hamre stated, "The foreign availability argument is seductive, but flawed." Strong encryption "is not, in fact, ubiquitously available overseas," he stated, adding that "we see no advantage in accelerating the general availability of such products to those who would wish us ill." Deputy Attorney General Jamie Gorelick testified in September 1996 that the availability of encryption software over the internet "does not undermine the utility of controls on exports of software or hardware products. The simple fact is that the majority of businesses and individuals with a serious need for strong encryption do not and will not rely on encryption downloaded from the internet." Lifting U.S. export controls, she argued, would "[damage] our own national security interests" and may not provide the expected benefits to industry if the removal of U.S. export controls leads to the introduction by other countries of import restrictions.

In spite of these national security concerns, controls over the export of U.S.-origin encryption products continued to be liberalized. In June 1997, Netscape Communications Corporation and Microsoft Corporation received permission to export encryption products up to 128 bits in length for use exclusively for banking and financial transactions. On September 16, 1998, the Administration announced a further relaxation of export controls on encryption. As part of this liberalization, the export of encryption products with key lengths up to 56 bits was completely decontrolled. Moreover, strong encryption products of any key length are now allowed to be exported, license-free, to several sectors of industry in 44 countries. These include subsidiaries of U.S. firms; insurance companies; health and medical organizations; and on-line merchants. The Administration also abandoned its insistence on development of a mandatory key recovery infrastructure.

H.R. 850, and companion legislation in the Senate, represent a further attempt to significantly liberalize U.S. encryption policy. In particular, H.R. 850 would:

(1) prohibit the government from requiring the use of key-recoverable encryption systems;

(2) prohibit the government from controlling the export or re-export of commercially-available encryption-capable software or computers using such software;

(3) grant the Commerce Department exclusive authority to control exports of all hardware, software, and technology for information security, except that designed for military use; and

(4) direct the Secretary of Commerce to allow the export or re-export of encryption-capable software for non-military end-uses in any country, or computers using such software based on considerations of foreign availability.

By prohibiting the government from requiring the use of key recovery-capable encryption products, section 2 of H.R. 850 would seriously impact the ability of the Department of Defense to effectively monitor the thousands of business and contract actions taken each day by the Department. In addition, this section would undermine government efforts to foster the voluntary development by industry of a key management infrastructure.

The committee notes that section 3 of H.R. 850 carries the most serious implications for U.S. national security. This section removes virtually all controls on the exportability of encryption products and greatly increases the likelihood that strong encryption products will be used by international terrorists to hide their plans. The committee notes that encryption is already being used by terrorists, and believes that the United States should not facilitate the spread of even stronger, unbreakable encryption capabilities to individuals or entities that seek to harm Americans. H.R. 850, as introduced, would do just that.

In his testimony before the committee on July 1, 1999, Deputy Secretary of Defense John Hamre stated, "I can unequivocally tell you Osama bin Laden (the accused mastermind of the U.S. Embassy bombings in Kenya and Tanzania) and other bad guys in the world are not only using information technology but encrypted information technology." Testifying before the committee on July 13, 1999, FBI Director Louis Freeh noted that Ramzi Yousef, convicted conspirator in the World Trade Center bombing, used encrypted computer files to mask his plans to blow up 11 U.S. airliners. It took "months and months" to decrypt that information. Director Freeh noted that "if those were plans that were imminent and we were in the possession of that [encrypted] information, we would not have been able to solve that."

The committee also notes that section 3 of H.R. 850 would remove all controls on the export of high-performance computers (so-called "supercomputers") if those computers contain encryption products or software that are "generally available." In the committee's view, this is one of the most significant and potentially dangerous flaws in H.R. 850. In light of the evidence that U.S. supercomputers were inappropriately transferred to entities of concern in Russia and China, and the recommendations to tighten export controls on high-performance computers contained in the report of the Congressionally-mandated Select Committee on U.S. National Security and Military/Commercial Concerns With the People's Republic of China (the "Cox Committee"), the removal of export re-

strictions on such machines would have significant consequences for U.S. national security. Further, this section would also supersede section 1211 of the National Defense Authorization Act for Fiscal Year 1998 (Public Law 105–85), which is designed to prevent the inadvertent export of supercomputers to questionable end users in countries of proliferation concern.

In summary, the committee concludes that H.R. 850, as introduced, would harm U.S. national security interests. According to Deputy Secretary of Defense Hamre, H.R. 850 "would seriously weaken our national security." In a March 24, 1999 letter to House Judiciary Committee Chairman Henry Hyde, Secretary Hamre stated, "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 * * *. H.R. 850 threatens our ability to do just that." In a May 24, 1999 letter to Chairman Spence, Secretary Hamre concluded that "H.R. 850 is anything but safe legislation." In his testimony before the committee on July 1, 1999, Secretary Hamre declared that the "unregulated release of the strongest encryption is going to do one thing: put more troops' lives at risk. Period." In her testimony before the committee on July 1, 1999, National Security Agency (NSA) Deputy Director McNamara testified that it will "greatly complicate our exploitation of foreign targets" and make NSA's job "difficult, if not impossible." She argued that "the immediate decontrol of encryption exports as proposed in the SAFE Act * * * [would] put national security at serious risk."

The committee notes that the Administration has also criticized the move to decontrol the export of encryption products on law-enforcement grounds. For example, in a July 16, 1999 letter to Chairman Spence, the President of the International Association of Chiefs of Police stated that H.R. 850 "would pose an enormous danger to both law enforcement and to society as a whole."

In response to these concerns, the committee agreed to amend H.R. 850 by deleting all after the enacting clause and substituting language that would grant the President authority to control exports of all dual-use encryption technology. The amendment also would allow for export without a license (referred to as a "license exception") for the export of encryption products with a strength at or below the maximum threshold established by the President. Export of these products would only occur under a "license exception" after a one-time government review. The President would also be able to waive an export under license exception for national security reasons. The amendment would also direct the President to notify Congress on a semi-annual basis of the appropriate threshold for the strength of encryption products that may be exported without harm to U.S. national security. The Congress would have a 30-day period to review the appropriateness of the notified level.

The amendment would establish licensing criteria for the export of encryption items with a strength that exceeds the maximum threshold established by the President for license exception. It would also be consistent with current Administration policy that allows the export of strong encryption to certain industry sectors, such as financial and medical institutions. In addition, the amend-

ment would establish an encryption industry and information security board to review and advise the President on the foreign availability of encryption products.

LEGISLATIVE HISTORY

H.R. 850, the "Security and Freedom through Encryption (SAFE) Act," was introduced by Representative Bob Goodlatte (R–VA) on February 25, 1999. The bill was reported April 27, 1999 by the House Committee on Judiciary (H. Report 106–117, Part I), and was reported (amended) on July 2, 1999 by the House Committee on Commerce (H. Rept. 106–117, Part II). The bill was also referred to the Committee on International Relations, the Permanent Select Committee on Intelligence, and the Committee on Armed Services.

On July 1, 1999 the Committee on Armed Services held a hearing on H.R. 850. Testimony was taken from Deputy Secretary of Defense John Hamre and Deputy Director of the National Security Agency Barbara McNamara. The focus of the hearing was to assess the bill's impact on U.S. national security.

On July 13, 1999, a second full committee hearing was held. Testimony was received from Attorney General Janet Reno, FBI Director Louis Freeh, Under Secretary of Commerce for Export Administration William Reinsch, and industry witnesses regarding the legislation's impact on national security, law enforcement, and public safety.

On July 21, 1999, the committee held a mark-up session to consider H.R. 850. The committee adopted an amendment in the nature of a substitute by a record vote of 47 to 6. The amended version of the bill was reported favorably by a voice vote. The record vote result can be found at the end of this report.

SECTION-BY-SECTION ANALYSIS

The following is a section-by-section analysis of the amendment in the nature of a substitute adopted by the committee.

Section 1—Short title

This section would cite the Act as the "Protection of National Security and Public Safety Act."

Section 2—Exports of encryption

This section would grant the President authority to control the export of all dual-use encryption products and would allow the President to deny the export of any encryption product if such export would be contrary to the national security interest. It would also ensure that any Presidential decision with respect to the export of encryption products is not subject to judicial review.

Section 3—License exception for certain encryption products

This section would allow an encryption product of a strength less than or equal to the threshold established by the President in section 5 to be exported without a license ("license exception") if certain conditions are met, including submission of the product for a one-time technical review.

Section 4—One-time product review

This section would require the President to specify the information that must be submitted for the one-time product review.

Section 5—Eligibility levels

This section would require the President to establish, within 180 days of enactment, the maximum level of encryption strength that may be exported under license exception without harm to U.S. national security interests. It would also require the President to review this threshold level every six months. In both cases, the level would not take effect until 30 days after the Congress is notified. In effect, this section would grant the President the flexibility to adjust the export licensing threshold as the level of technology advances, consistent with U.S. national security requirements.

Section 6—Encryption licenses required

This section would require an export license for an encryption product with a strength that exceeds the threshold level established by the President in section 5. It would require an exporter seeking an export license to submit the encryption product for technical review and to provide a certification identifying the intended end use and end user of the product. In instances where the export is to a distribution chain partner, it would require submission of the name and address of the partner, along with proof that the partner has contractually agreed to abide by all U.S. export and reexport laws and regulations. This section would also require exporters to notify the Secretary of Commerce if they have reason to believe that their encryption product is being used in an unapproved manner or by an unapproved end user. This section would also require distribution chain partners to submit a report on the intended end use and end user of the product.

Section 7—Waiver authority

This section would allow the President to waive the license exception requirements in section 3 for national security reasons. It would also allow the President to exempt certain industry sectors from the licensing requirements in section 6 after notifying Congress. This would be consistent with current Administration policy which allows the unlicensed export of strong encryption products to certain sectors of industry, such as financial and medical institutions.

Section 8—Encryption industry and information security board

This section would establish an advisory board to review and advise the President on the foreign availability of encryption products. The board would be composed of six government officials and six members from the private sector. The findings of the board would be conveyed to the President and the Congress.

Section 9—Market share survey

This section would require the Secretary of Commerce to conduct, at least once every six months, a market share survey of foreign markets for encryption products.

Section 10—Definitions

This section would define terms used in this Act.

COMMITTEE POSITION

On July 21, 1999, the Committee on Armed Services, a quorum being present, approved H.R. 850 as amended, by a voice vote.

FISCAL DATA

Pursuant to clause 3(d)(2)(A) of rule XIII of the Rules of the House of Representatives, the committee attempted to ascertain annual outlays resulting from the bill during fiscal year 2000 and the four following fiscal years. The results of such efforts are reflected in the cost estimate prepared by the Director of the Congressional Budget Office under section 402 of the Congressional Budget Act of 1974, which is included in this report pursuant to clause 3(c)(3) of rule XIII of the Rules of the House.

Congressional Budget Office Estimate

In compliance with clause 3(c)(3) of rule XIII of the Rules of the House of Representatives, the cost estimate prepared by the Congressional Budget Office and submitted pursuant to section 402(a) of the Congressional Budget Act of 1974 is as follows:

JULY 22, 1999.

Hon. FLOYD SPENCE,
Chairman, Committee on Armed Services,
House of Representatives, Washington, DC.

DEAR MR. CHAIRMAN: The Congressional Budget Office has prepared the enclosed cost estimate for H.R. 850, the Protection of National Security and Public Safety Act.

If you wish further details on this estimate, we will be pleased to provide them. The CBO staff contact is Mark Hadley.

Sincerely,

DAN L. CRIPPEN, *Director.*

CONGRESSIONAL BUDGET OFFICE COST ESTIMATE

Protection of National Security and Public Safety Act

H.R. 850 would clarify the President's authority to control the export of encryption products. The effectiveness or strength of contemporary encryption products is measured by the number of bits that make up the key for the encryption algorithm. (The term "key" refers to the mathematical code used to translate encrypted information back into its original, unencrypted format.) Under current policy, domestic producers may export encryption products with key lengths of up to 56 bits and stronger products for specified industries.

Under the bill, the President would determine the maximum strength of encryption products that may be exported (with review and potential updates of that maximum every 180 days). In addition, the bill would allow the President to deny the export of any encryption product if the export of such product is contrary to the national security interest of the United States. H.R. 850 would establish a board to advise the President on the export of encryption

products. Finally, the bill would require the Department of Commerce to conduct a market share survey of foreign markets for encryption products every six months.

Based on information from the Department of Commerce, CBO estimates that implementing H.R. 850 would cost about $1 million a year, subject to appropriation of the necessary mounts. H.R. 850 would not affect direct spending or receipts; therefore, pay-as-you-go procedures would not apply. H.R. 850 contains no intergovernmental or private-sector mandates as defined in the Unfunded Mandates Reform Act and would impose no costs on state, local, or tribal governments.

CBO has completed numerous other estimates of bills affecting the export of encryption products, including three versions of H.R. 850. Differences between this estimate and our previous estimates reflect differences between the bills. On April 21, 1999, CBO transmitted a cost estimate for H.R. 850 as ordered reported by the House Committee on the Judiciary on March 24, 1999. On July 1, 1999, CBO transmitted an estimate for H.R. 850 as ordered reported by the House Committee on Commerce on June 23, 1999. On July 16, 1999, CBO transmitted an estimate of H.R. 850 as ordered reported by the House Committee on International Relations on July 13, 1999. And on July 9, 1999, CBO transmitted an estimate for S. 798, the Promote Reliable Online Transactions to Encourage Commerce and Trade (PROTECT) Act of 1999, as ordered reported by the Senate Committee on Commerce, Science, and Transportation on June 23, 1999. CBO estimated that the versions reported by the Judiciary Committee and the International Relations Committee would each cost between $3 million and $5 million over the 2000–2004 period and that the House Commerce Committee's version of H.R. 850 and the Senate bill (S. 798) would each increase costs by at least $25 million over the same period.

The CBO staff contact is Mark Hadley. This estimate was approved by Robert A. Sunshine, Deputy Assistant Director for Budget Analysis.

Committee cost estimate

Pursuant to clause 3(d) of rule XIII of the Rules of the House of Representatives, the committee generally concurs with the estimate contained in the report of the Congressional Budget Office.

OVERSIGHT FINDINGS

With respect to clause 3(c)(1) of rule XIII of the Rules of the House of Representatives, this legislation results from hearings and other oversight activities conducted by the committee pursuant to clause 2(b)(1) of rule X.

With respect to clause 3(c)(2) of rule XIII of the Rules of the House of Representatives and section 308(a)(1) of the Congressional Budget Act of 1974, this legislation does not include any new spending or credit authority, nor does it provide for any increase or decrease in tax revenues or expenditures. The fiscal features of this legislation are addressed in the estimate prepared by the Director of the Congressional Budget Office under section 402 of the Congressional Budget Act of 1974.

With respect to clause 3(c)(4) of rule XIII of the Rules of the House of Representatives, the committee has not received a report from the Committee on Government Reform and Oversight pertaining to the subject matter of H.R. 850.

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 United States Constitution.

STATEMENT OF FEDERAL MANDATES

Pursuant to section 423 of Public Law 104–4, this legislation contains no federal mandates with respect to state, local, and tribal governments, nor with respect to the private sector. Similarly, the bill provides no unfunded federal intergovernmental mandates.

RECORD VOTE

In accordance with clause 3(b) of rule XIII of the Rules of the House of Representatives, a record vote was taken with respect to the committee's consideration of H.R. 850. The record of this vote can be found on the following page.

The committee ordered H.R. 850, as amended, reported to the House with a favorable recommendation by a voice vote, a quorum being present.

COMMITTEE ON ARMED SERVICES
106TH CONGRESS
RECORD VOTE

Description: Amendment in the Nature of a Substitute

Date: July 21, 1999

Offered by: Mr. Weldon, Mr. Sisisky and Mr. Andrews

Voice Vote Ayes Nays

Rep.	Aye	Nay	Present	Rep.	Aye	Nay	Present
Mr. Spence	X			Mr. Skelton	X		
Mr. Stump	X			Mr. Sisisky	X		
Mr. Hunter	X			Mr. Spratt	X		
Mr. Kasich	X			Mr. Ortiz	X		
Mr. Bateman	X			Mr. Pickett	X		
Mr. Hansen	X			Mr. Evans	X		
Mr. Weldon	X			Mr. Taylor	X		
Mr. Hefley	X			Mr. Abercrombie	X		
Mr. Saxton	X			Mr. Meehan		X	
Mr. Buyer	X			Mr. Underwood	X		
Mrs. Fowler	X			Mr. Kennedy			
Mr. McHugh	X			Mr. Blagojevich	X		
Mr. Talent				Mr. Reyes	X		
Mr. Everett	X			Mr. Allen	X		
Mr. Bartlett	X			Mr. Snyder	X		
Mr. McKeon	X			Mr. Turner	X		
Mr. Watts	X			Mr. Smith		X	
Mr. Thornberry				Ms. Sanchez		X	
Mr. Hostettler	X			Mr. Maloney	X		
Mr. Chambliss	X			Mr. McIntyre	X		
Mr. Hilleary	X			Mr. Rodriguez			
Mr. Scarborough				Ms. McKinney			
Mr. Jones	X			Ms. Tauscher		X	
Mr. Graham	X			Mr. Brady	X		
Mr. Ryun	X			Mr. Andrews	X		
Mr. Riley	X			Mr. Hill		X	
Mr. Gibbons				Mr. Thompson	X		
Ms. Bono		X		Mr. Larson	X		
Mr. Pitts	X						
Mr. Hayes	X						
Mr. Kuykendall	X						
Mr. Sherwood	X						

Roll Call Vote Total 47 Aye 6 Nay Present

ADDITIONAL VIEWS

Mr. Chairman, I submit the following additional comments for inclusion to the committee report for H.R. 850 and thank you for your considerations.

As an original co-sponsor of the Security and Freedom Through Encryption Act (SAFE) I demonstrated my support for an open market. It is my belief that we can and should be the world's leader in the development and marketing of technologies, and as a member of Congress we have a responsibility to protect the security of the American people.

The amended version of H.R. 850 is the first step to take a serious look at what is required to release technologies and protect National Security. I look forward to continued discussions on this issue and the establishment of a performance threshold for encryption that will serve both the private and public sector.

J.C. WATTS, Jr.

SUPPLEMENTAL VIEWS

As a Member of the House Armed Services Committee, I am the first to stand in support of our national security. But now is the time to legislate a balanced encryption policy in the United States.

Over the course of the 106th Congress, I have met with and talked to numerous experts in the computer and security field. The experts I spoke with represented various views on export controls to encode, or encrypt, electronic communications. Now is the time for Congress to make a decision for a well thought out encryption policy for this great country of ours.

It is my belief, that current U.S. regulations limit the export of encryption and unfairly handicap American high-technology companies. Even though we are the leaders in information technology, it is vital that we maintain our strategic information dominance. What is imperative is that our law enforcement and national security agencies must do more to develop alternative means for achieving their missions while focusing on strong encryption.

The provisions of the SAFE Act would remove most license requirements for exports of recoverable products. It would remove existing barriers to secure e-commerce and business-to-business transactions. The SAFE Act, however, would not absolve the computer industry of its obligations, to law enforcement, or to the intelligence community.

We all acknowledge that the United States leads the world in the production of computer hardware and software, and technology is the engine driving the global economy. We as a country, should not sit idly by and let U.S. companies lose their edge in the world market because they can't deliver the kind of secure products and services that customers demand.

H.R. 850 ensures that safety and security become the cornerstones of the information superhighway. If U.S. encryption continues to be restricted, foreign products may soon dominate the worldwide market, hindering our ability to gather intelligence against terrorists and criminals.

I would also like to state for the record that for reasons stated above, I would not have voted for the Weldon, Sisisky, and Andrews Substitute Amendment, had I been present.

PATRICK J. KENNEDY.

Document No. 16