105TH CONGRESS
1st Session

HOUSE OF REPRESENTATIVES

REPT. 105–108
Part 3

SECURITY AND FREEDOM THROUGH ENCRYPTION (SAFE) ACT OF 1997

R E P O R T

OF THE

COMMITTEE ON NATIONAL SECURITY HOUSE OF REPRESENTATIVES

ON

H.R. 695

together with

ADDITIONAL AND SUPPLEMENTAL VIEWS

[Including cost estimate of the Congressional Budget Office]

SEPTEMBER 12, 1997.—Ordered to be printed

U.S. GOVERNMENT PRINTING OFFICE
43–310 WASHINGTON : 1997

HOUSE COMMITTEE ON NATIONAL SECURITY

ONE HUNDRED FIFTH CONGRESS

FLOYD D. SPENCE, South Carolina, *Chairman*

BOB STUMP, Arizona
DUNCAN HUNTER, California
JOHN R. KASICH, Ohio
HERBERT H. BATEMAN, Virginia
JAMES V. HANSEN, Utah
CURT WELDON, Pennsylvania
JOEL HEFLEY, Colorado
JIM SAXTON, New Jersey
STEVE BUYER, Indiana
TILLIE K. FOWLER, Florida
JOHN M. MCHUGH, New York
JAMES TALENT, Missouri
TERRY EVERETT, Alabama
ROSCOE G. BARTLETT, Maryland
HOWARD "BUCK" MCKEON, California
RON LEWIS, Kentucky
J.C. WATTS, JR., Oklahoma
MAC THORNBERRY, Texas
JOHN N. HOSTETTLER, Indiana
SAXBY CHAMBLISS, Georgia
VAN HILLEARY, Tennessee
JOE SCARBOROUGH, Florida
WALTER B. JONES, JR., North Carolina
LINDSEY GRAHAM, South Carolina
SONNY BONO, California
JIM RYUN, Kansas
MICHAEL PAPPAS, New Jersey
BOB RILEY, Alabama
JIM GIBBONS, Nevada
BILL REDMOND, New Mexico

RONALD V. DELLUMS, California
IKE SKELTON, Missouri
NORMAN SISISKY, Virginia
JOHN M. SPRATT, JR., South Carolina
SOLOMON P. ORTIZ, Texas
OWEN PICKETT, Virginia
LANE EVANS, Illinois
GENE TAYLOR, Mississippi
NEIL ABERCROMBIE, Hawaii
MARTIN T. MEEHAN, Massachusetts
ROBERT A. UNDERWOOD, Guam
JANE HARMAN, California
PAUL MCHALE, Pennsylvania
PATRICK J. KENNEDY, Rhode Island
ROD R. BLAGOJEVICH, Illinois
SILVESTRE REYES, Texas
TOM ALLEN, Maine
VIC SNYDER, Arkansas
JIM TURNER, Texas
F. ALLEN BOYD, JR., Florida
ADAM SMITH, Washington
LORETTA SANCHEZ, California
JAMES H. MALONEY, Connecticut
MIKE MCINTYRE, North Carolina
CIRO D. RODRIGUEZ, Texas
CYNTHIA A. MCKINNEY, Georgia

ANDREW K. ELLIS, *Staff Director*

CONTENTS

105TH CONGRESS *1st Session* } HOUSE OF REPRESENTATIVES { REPT. 105–108 Part 3

SECURITY AND FREEDOM THROUGH ENCRYPTION (SAFE) ACT OF 1997

SEPTEMBER 12, 1997.—Ordered to be printed

Mr. SPENCE, from the Committee on National Security, submitted the following

R E P O R T

together with

ADDITIONAL AND SUPPLEMENTAL VIEWS

[To accompany H.R. 695]

[Including cost estimate of the Congressional Budget Office]

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

The amendments are as follows:

Strike section 3 and insert the following:

SEC. 3. EXPORTS OF ENCRYPTION.

(a) EXPORT CONTROL OF ENCRYPTION PRODUCTS NOT CONTROLLED ON THE UNITED STATES MUNITIONS LIST.—The Secretary of Commerce, with the concurrence of the Secretary of Defense, shall have the authority to control the export of encryption products not controlled on the United States Munitions List. Decisions made by the Secretary of Commerce with the concurrence of the Secretary of Defense with respect to exports of encryption products under this section shall not be subject to judicial review.

(b) LICENSE EXCEPTION FOR CERTAIN ENCRYPTION PRODUCTS.—Encryption products with encryption strength equal to or less than the level identified in subsection (d) shall be eligible for export under a license exception after

a 1-time review, if the encryption product being exported does not include features that would otherwise require licensing under applicable regulations, is not destined for countries, end-users, or end-uses that the Secretary of Commerce has determined by regulation, with the concurrence of the Secretary of Defense, are ineligible to receive such products, and is otherwise qualified for export.

(c) ONE-TIME PRODUCT REVIEW.—The Secretary of Commerce, with the concurrence of the Secretary of Defense, shall specify the information that must be submitted for the 1-time review referred to in subsection (b).

(d) ELIGIBLE ENCRYPTION LEVELS.—

(1) INITIAL ELIGIBILITY LEVEL.—Not later than 30 days after the date of the enactment of this Act, the President shall notify the Congress of the maximum level of encryption strength that could be exported from the United States under license exception pursuant to this section without harm to the national security of the United States. Such level shall not become effective until 60 days after such notification.

(2) ANNUAL REVIEW OF ELIGIBILITY LEVEL.—Not later than 1 year after notifying the Congress of the maximum level of encryption strength under paragraph (1), and annually thereafter, the President shall notify the Congress of the maximum level of encryption strength that could be exported from the United States under license exception pursuant to this section without harm to the national security of the United States. Such level shall not become effective until 60 days after such notification.

(3) CALCULATION OF 60-DAY PERIOD.—The 60-day period referred to in paragraphs (1) and (2) shall be computed by excluding—

(A) the days on which either House is not in session because of an adjournment of more than 3 days to a day certain or an adjournment of the Congress sine die; and

(B) each Saturday and Sunday, not excluded under subparagraph (A), when either House is not in session.

(e) EXCERCISE OF EXISTING AUTHORITIES.—The Secretary of Commerce and the Secretary of Defense may exercise the authorities they have under other provisions of law to carry out this section.

Amend the title so as to read:

A bill to amend title 18, United States Code, to affirm the rights of United States persons to use and sell encryption.

PURPOSE AND BACKGROUND

The explosive growth of the internet and the rise in electronic commerce in recent years have led to increased concerns over information security. A growing number of individuals and businesses now have access to the information superhighway and the capabil-

ity 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. Industry has responded to this risk by developing products with 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 the personal information they send will be protected.

Currently, the domestic use of encryption products is unrestricted. When used by law-abiding citizens and companies, encryption can increase public confidence in the security of electronic transactions. However, the export of encryption capabilities is controlled for important national security and foreign policy reasons. 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. Moreover, much of the U.S. military's battlefield advantage relies on information dominance and the ability to decipher enemy communications. Unrestricted export of capabilities that make it more difficult for the United States to comprehend the plans and activities of hostile military forces could significantly degrade the technological advantage presently held by U.S. combat forces.

In particular, the committee notes that the U.S. military has made information warfare a key element of U.S. military strategy and tactics. U.S. strategy requires that the United States be able to protect its own communications from interception while exploiting the weaknesses in the information systems and communications of potential adversaries. The National Defense University Institute for National Strategic Studies 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," potentially leading to the prompt termination of conflict and a reduction in civilian and military casualties. However, the committee is concerned that the proliferation of sophisticated encryption capabilities overseas may

make it more difficult for the United States to maintain its military superiority and achieve tactical battlefield advantages.

Because of national security implications, the United States has traditionally considered encryption products to be sensitive "munitions" items and their export has been carefully controlled by the Department of State. However, in October 1996, the Clinton Administration decided to transfer jurisdiction over the export of commercial encryption products from the Department of State to the Department of Commerce, 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 keys by government law-enforcement agents or intelligence officials, if necessary, in order to decode scrambled information.

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." Prior to this decision, U.S. policy allowed the unrestricted export of encryption software with keys up to 40 bits in length.

In announcing this 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."

As received by the committee, H.R. 695 and companion legislation in the Senate represent a further attempt to significantly liberalize U.S. encryption policy. In particular, H.R. 695, as introduced, would have the following effect on encryption export controls:

(1) It would grant the Commerce Department exclusive authority to control exports of all hardware, software, and technology for information security, except that designed for military use, depriving the Secretary of Defense of an appropriate level of involvement on licensing decisions involving national security;

(2) It would prohibit requiring a government-validated license for the export or re-export of commercially-available encryption-capable software or computers using such software; and

(3) It would 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.

Importantly, the committee notes that section 3 of H.R. 695 would require the government to approve exports of high performance computers (so-called "supercomputers") if those computers contain encryption products or software that are commercially available. In the committee's view, this is one of the most serious consequences and flaws of the bill. Under this proposed arrangement, any company would be in a position to force the government to allow the export of even the most powerful supercomputer available in the United States, if they first loaded a piece of foreign-available encryption software on the supercomputer. As confirmed by Secretary Reinsch in his testimony before the committee, this provision would overturn the Spence-Dellums amendment to H.R. 1119, the National Defense Authorization Act for Fiscal Year 1997, adopted by the House on June 19, 1997, by a vote of 332–88. That amendment would prevent the inadvertent export of supercomputers to questionable end users in countries of proliferation concern.

The committee believes that the provisions of H.R. 695, as introduced, in particular those provisions regarding export controls on encryption products, do not adequately address these significant national security concerns. In testimony before the committee on July 30, 1997, Under Secretary of Commerce for Export Administration William Reinsch stated that H.R. 695 "proposes export liberalization far beyond what the administration can entertain and which we believe would be contrary to our international export control obligations and detrimental to our national security." With respect to the bill's national security implications, William Crowell, Deputy Director of the National Security Agency (NSA), testified that "the passage of H.R. 695 would negatively impact NSA's missions. * * * the immediate decontrol of strong encryption products without restriction would make our signals intelligence mission much more difficult and ultimately result in the loss of intelligence. * * * This would greatly complicate our exploitation of foreign targets, including military targets." Mr. Crowell concluded that H.R. 695 "will do irreparable harm to national security. * * *"

The Administration also has criticized H.R. 695 on broader grounds. For example, the Federal Bureau of Investigation has declared that "it would be irresponsible for the U.S. to adopt a policy that consciously unleashes widespread, unbreakable, non-key recovery encryption products that undermine law enforcement in the United States and worldwide." According to the Department of Defense, H.R. 695 would "have a negative impact on national security, effective law enforcement and public safety." The Director of the National Security Agency, Lieutenant General Kenneth A. Minihan, has noted that the United States obtains "a substantial amount of significant intelligence information from unencrypted sources" and that this information is "likely to become encrypted with the relaxation of crypto export controls." In a recent letter to Chairman Spence and Ranking Member Dellums, Secretary of Defense Cohen stated, "Passage of legislation which effectively decontrols commercial encryption exports would undermine U.S. efforts"

to foster a key recovery infrastructure that will "preserve governments' abilities to counter worldwide terrorism, narcotics trafficking and proliferation."

In response to these concerns, the committee agreed to amend section 3 of H.R. 695, the section of the bill dealing with export controls. Given the committee's jurisdictional focus on national security, the committee exclusively limited its actions to this section of the bill and did not address the effects of H.R. 695 on domestic law enforcement capabilities. The committee amendment to section 3 would allow the President, subject to 60 day congressional review, to determine the maximum level of encryption strength that may be exported without a license. Unlicensed export of these products could occur after a one-time review. Products above the threshold could be exported under an individually validated license, and the committee's amendment ensures that the concurrence of the Secretary of Defense is obtained prior to the export of such more sophisticated encryption software. The amendment also ensures that the appropriateness of the threshold level would be reviewed on an annual basis.

LEGISLATIVE HISTORY

H.R. 695, the "Security and Freedom through Encryption (SAFE) Act of 1997," was introduced by Representative Robert Goodlatte (R–VA) on February 12, 1997. The bill was reported in May 1997 by the House Committee on the Judiciary. The bill was also referred to the Committee on International Relations, the Committee on Commerce, the Permanent Select Committee on Intelligence, and the Committee on National Security. On July 22, 1997, the House International Relations Committee approved the bill with minor amendments.

On July 30, 1997, the Committee on National Security held a hearing on H.R. 695. Testimony was taken from representatives of the Department of Defense, Department of Commerce, and industry witnesses. The focus of the hearing was to assess the bill's impact on U.S. national security.

On September 9, 1997, the committee held a mark-up session to consider H.R. 695. The committee adopted one amendment to the bill dealing with Section 3 on export controls by a rollcall vote of 45 to 1. The amended version of the bill was reported favorably by a voice vote. The individual rollcall result is placed at the end of this report.

SECTION-BY-SECTION ANALYSIS

SECTION 1—SHORT TITLE

This section would establish a short title of the bill as the "Security and Freedom Through Encryption (SAFE) Act."

SECTION 2—SALE AND USE OF ENCRYPTION

This section would amend Part I of title 18, United States Code by adding a new chapter on "Encrypted Wire and Electronic Communications" consisting of five sections. This new chapter would define encryption and related terms, legalize the use of any

encryption method by U.S. citizens domestically or abroad, and legalize the interstate sale by U.S. citizens of any encryption, regardless of algorithm or key length. The new chapter would also deny any person the right to control a key that is in the lawful possession of another person, except for law enforcement purposes, thereby nullifying the government's key escrow plan. Finally, the new chapter would establish penalties for the unlawful use of encryption in furtherance of a criminal act.

SECTION 3—EXPORTS OF ENCRYPTION

As amended, this section would grant the Secretary of Commerce authority, with the concurrence of the Secretary of Defense, to control exports of encryption technology that is not controlled on the U.S. Munitions List. The section also would allow for 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 after a one-time government review. The export of encryption products with a strength above the threshold determined by the President would be allowed subject to existing regulations and procedures. The amendment would not impact the current ability of financial institutions to export encryption products above the threshold without limitation, for use exclusively for banking and financial transactions. This section would also direct the President to notify Congress on an annual basis of the appropriate threshold for the strength of encryption products that may be exported without harm to U.S. national security. Current civil and criminal penalties for violation of U.S. export control restrictions would continue to apply, and would cover the procedures established in the committee's amendment.

COMMITTEE POSITION

On September 9, 1997, the Committee on National Security, a quorum being present, approved H.R. 695, as amended, by a voice vote.

FISCAL DATA

Pursuant to clause 7 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 1998 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 403 of the Congressional Budget Act of 1974, which is included in this report pursuant to clause 2(l)(3)(C) of House rule XI.

CONGRESSIONAL BUDGET OFFICE ESTIMATE

In compliance with clause 2(l)(3)(C) of rule XI of the Rules of the House of Representatives, the cost estimate prepared by the Congressional Budget Office and submitted pursuant to section 403(a) of the Congressional Budget Act of 1974 is as follows:

SEPTEMBER 11, 1997.

Hon. FLOYD SPENCE,
Chairman, Committee on National Security,
House of Representatives, Washington, DC.

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

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

Sincerely,

JUNE E. O'NEILL, *Director.*

CONGRESSIONAL BUDGET COST OFFICE ESTIMATE

Summary: H.R. 695 would allow individuals in the United States to use or sell any encryption product 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 authorize the President to determine which encryption products could be granted an export license exception and thus could be exported following a one-time product review by the Department of Commerce's Bureau of Export Administration (BXA). Other encryption products would be subject to more stringent export controls imposed by the Secretary of Commerce with the concurrence of the Secretary of Defense. H.R. 695 would establish criminal penalties and fines for the use of encryption technologies to conceal from law enforcement officials incriminating information relating to a crime.

CBO estimates that implementing this bill would not add to BXA's costs of reviewing encryption products intended for export. Both under current policies and under the provisions of H.R. 695, CBO estimates that spending by BXA for reviewing the export of nonmilitary encryption products would total about $4.5 million over the 1998–2000 period.

The bill would affect direct spending and receipts beginning in fiscal year 1998 through the imposition of criminal fines and the resulting spending from the Crime Victims Fund. Therefore, pay-as-you-go procedures would apply. CBO estimates, however, that the amounts of additional direct spending and receipts would not be significant.

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

Estimated cost to the Federal Government

In November 1996, the Administration issued an executive order and memorandum that authorized the export of encryption products up to 56 bits in length following a one-time product review by BXA, contingent on the exporter's commitment to develop a key recovery system. H.R. 695 would maintain the President's discretion

to determine which encryption products could be exported following a one-time review by BXA and which products would be subject to more stringent export controls by the agency. Based on information from BXA, CBO expects that the President would not modify the current policy of allowing license exceptions for encryption products of up to 56 bits in length. Thus, enacting this bill would not significantly change the scope of BXA's activities. Assuming appropriation of the necessary amounts, CBO estimates that implementing H.R. 695 would result in costs to BXA of about $900,000 in each fiscal year, totaling about $4.5 million over the 1998–2002 period, about the same as would be expected under current law. BXA was authorized to spend $850,000 in fiscal year 1997 to control encryption exports.

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

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

Pay-as-you-go considerations

Section 252 of the Balanced Budget and Emergency Deficit Control Act of 1985 sets up pay-as-you-go procedures for legislation affecting direct spending or receipts. H.R. 695 would affect direct spending and receipts through the imposition of criminal fines and the resulting spending from the Crime Victims Fund. CBO estimates, however, that any collections and spending resulting from such fines would not be significant.

Estimated impact on state, local, and tribal governments

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

Estimated impact on the private sector

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

Previous CBO estimate

CBO provided cost estimates for H.R. 695 as ordered reported by the House Committee on the Judiciary on May 14, 1997, and as ordered reported by the House Committee on International Relations on July 22, 1997. Assuming appropriation of the necessary amounts, CBO estimates that implementing the Judiciary Commit-

tee's version of the bill would cost between $5 million and $7 million over the 1998–2002 period and that implementing the International Relations Committee's version would cost about $2.2 million over the same period. The estimated cost under current policies and for the National Security Committee's version is $4.5 million.

Estimate prepared by: Federal Costs: Rachel Forward, Revenues: Alyssa Trzeszkowski, Impact on State, Local, and Tribal Governments: Pepper Santalucia.

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

COMMITTEE COST ESTIMATE

Pursuant to Clause 7(a) 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.

INFLATION IMPACT STATEMENT

Pursuant to clause 2(l)(4) of rule XI of the Rules of the House of Representatives, the committee concludes that the bill would have no significant inflationary impact.

OVERSIGHT FINDINGS

With respect to clause 2(l)(3)(A) of rule XI 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 2(l)(3)(B) of rule XI 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 403 of the Congressional Budget Act of 1974.

With respect to clause 2(l)(3)(D) of rule XI 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. 695.

CONSTITUTIONAL AUTHORITY STATEMENT

Pursuant to clause 2(l)(4) of rule XI 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.

ROLLCALL VOTE

In accordance with clause 2(l)(2)(B) of rule XI of the Rules of the House of Representatives, a rollcall vote was taken with respect to the committee's consideration of H.R. 695. The record of this vote is attached to this report.

The committee ordered H.R. 695, as amended, reported to the House with a favorable recommendation by a voice vote, a quorum being present.

COMMITTEE ON NATIONAL SECURITY
105TH CONGRESS
ROLL CALL

Date: 09/09/97
Offered By: Mr. Weldon and Mr. Dellums

Rep.	Aye	Nay	Present	Rep.	Aye	Nay	Present
Mr. Spence	X			Mr. Dellums			
Mr. Stump				Mr. Skelton	X		
Mr. Hunter	X			Mr. Sisisky	X		
Mr. Kasich				Mr. Spratt	X		
Mr. Bateman	X			Mr. Ortiz	X		
Mr. Hansen				Mr. Pickett	X		
Mr. Weldon	X			Mr. Evans	X		
Mr. Hefley	X			Mr. Taylor	X		
Mr. Saxton	X			Mr. Abercrombie	X		
Mr. Buyer	X			Mr. Meehan			
Mrs. Fowler	X			Mr. Underwood			
Mr. McHugh	X			Ms. Harman	X		
Mr. Talent	X			Mr. McHale	X		
Mr. Everett	X			Mr. Kennedy	X		
Mr. Bartlett	X			Mr. Blagojevich	X		
Mr. McKeon	X			Mr. Reyes	X		
Mr. Lewis	X			Mr. Allen	X		
Mr. Watts	X			Mr. Snyder	X		
Mr. Thornberry	X			Mr. Turner	X		
Mr. Hostettler	X			Mr. Boyd	X		
Mr. Chambliss	X			Mr. Smith		X	
Mr. Hilleary	X			Ms. Sanchez			
Mr. Scarborough				Mr. Maloney	X		
Mr. Jones				Mr. McIntyre			
Mr. Graham	X			Mr. Rodriguez			
Mr. Bono	X			Ms. McKinney	X		
Mr. Ryun	X						
Mr. Pappas	X						
Mr. Riley	X						
Mr. Gibbons	X						
Mr. Redmond	X						

Roll Call Vote Total **45 Aye** **1 Nay** **Present**

CHANGES IN EXISTING LAW MADE BY THE BILL, AS REPORTED

The bill was referred to this committee for consideration of such provisions of the bill as fall within the jurisdiction of this committee pursuant to clause 1(k) of rule X of the Rules of the House of Representatives. The changes made to existing law by the amendment reported by the Committee on the Judiciary are shown in the report filed by that committee (Rept. 105–108, Part 1). The amendments made by this committee do not make any changes in existing law.

ADDITIONAL VIEWS OF CONGRESSMAN PATRICK J. KENNEDY

Mr. Chairman, as a member of the House National Security Committee for almost three years, I have voted in favor of research and development of advanced technology, I have supported procurement of state of the art weapons systems and I have advocated greater funding for training and educating our armed forces. I am proud of the role our committee plays in working to ensure our men and women in uniform are properly equipped to meet the many challenges and missions our nation asks of them. After having received a classified briefing by the National Security Agency, I now believe that if we support H.R. 695, the "Security and Freedom through Encryption Act", as introduced, we would effectively nullify the many important national security investments made by this committee.

Let me be clear, I support providing American businesses the opportunity to be competitive in the export of encryption products but I also understand the importance of limited export controls to the intelligence community and to our country's national security. Our national security and our economic interests should not be interpreted as mutually exclusive. I am convinced that any legislation we pass must strike a balance between our national security concerns and our economic interests. Unfortunately, H.R. 695, as introduced, fails to strike this balance. Rather than providing a means to assess the impact of encryption exports on our national security, this bill opens the floodgates and threatens to overwhelm our intelligence infrastructure.

I do believe that if we make modifications to H.R. 695, it is entirely possible to address some of the more important security and economic concerns The amendment offered today by Mr. Weldon and Mr. Dellums provides us that chance. The Weldon-Dellums amendment does not prevent or stop the export of encryption products. Rather than the immediate decontrol of strong encryption products which would come with H.R. 695, the amendment proposes responsible limits for the export of encryption technology, limits which are in part determined by a product's threat to national security.

The limits are necessary given the fact that today, a significant portion of the intelligence we collect is not encrypted. That information we glean is vital to threat warning, attack assessment and gaining tactical/information supremacy. Should our adversaries suddenly have access to strong encryption products, our intelligence community would be hampered and severely overwhelmed. Instantly we would put in jeopardy our ability to decode and decipher information from the predominant threats our country faces today: terrorist organizations, rogue nations and drug traffickers.

It is important to keep in mind that the limits included in the amendment are not permanent. The Administration would be forced to re-evaluate threshold levels every year in order to keep pace with technology. The Congress would then have the opportunity to review the appropriateness of the level and enact legislation to respond should it so choose. By ensuring that the threshold is reviewed on an annual basis, a process is created whereby we can assess the impact of the exports on our intelligence gathering and assessment capabilities while also providing a mechanism to alter the limits when conditions permit.

Both Mr. Weldon and Mr. Dellums should be commended for their hard work in crafting a bipartisan amendment to H.R. 695, an amendment which seeks to find that delicate balance between our national security requirements and ensuring our companies are provided the opportunity to compete.

PATRICK J. KENNEDY.

SUPPLEMENTAL VIEWS OF HON. JANE HARMAN

The debate over H.R. 695 and encryption has shed invaluable light on the difficult choices policy makers have to make in fashioning a policy where national security concerns and U.S. international competitiveness come into direct conflict. To be sure, our nation's security must be preeminent, and I don't doubt from the committee's hearings on the bill and from my conversations that the individuals and the companies which comprise the computer software industry designing encryption agree with this assessment.

At the same time, policy makers cannot let security concerns unduly restrict the ability of a vibrant and growing segment of our economy to compete on international markets—markets which they currently and rightly dominate. In our zeal to protect technologies which have defense and law enforcement implications, we should not adopt policies that stifle our own domestic enterprises and hand the lead to foreign entities beyond our own laws.

How we balance these competing goals, albeit not equally so, is the objective of the amendment offered by my colleagues, Mr. Weldon and Mr. Dellums, which the committee approved as a substitute to the original title 3 of H.R. 695. I support their objective, but am not persuaded that a revision in our export control policy is the best means of achieving it. In voting for the substitute amendment during the committee's mark-up, I outlined some reservations and would like at this time to offer some suggestions that would in my view, improve the approach the bill takes.

First, encourage, if not direct, the Administration to engage other countries on this issue. Given the availability of this technology abroad, and the ease of its dissemination, a unilateral export control policy on encryption will not work. We must work out a multilateral approach.

Second, drop the requirement that the Secretary of Commerce must have the concurrence of the Secretary of Defense to grant a license exception. Including this requirement is a step backwards from current policy. Under current export control policy there is a mechanism by which national security agencies like the Department of Defense can raise specific concerns with the Commerce Department as it reviews export license applications. No evidence has been presented to suggest that the current mechanism is broken and it should be used for encryption export licenses as well. Giving the DoD what is in effect a veto may result in the denial of export licenses for otherwise eligible encryption products.

Third, provide guidance or outline specific criteria for the President to use in setting the maximum level of encryption below which license exceptions would be granted. Encryption technology develops rapidly and we need to ensure that advances made both domestically and abroad are taken into consideration so that U.S. companies are not penalized by the setting of an artificially low

encryption strength level. As such, the committee should at minimum specifically require the President to conduct a rigorous assessment of the range and quality of encryption products available in foreign markets and require he explain why that should not be the maximum strength level.

Fourth, set forth a specific period of time within which companies seeking license exceptions for their products can expect to have their application reviewed and either approved or rejected. During this time frame, the relevant federal agencies could examine the encryption technology in question and have the applicant respond to any national security concerns the technology raises. It is important that this period of time be narrowly defined, in order to assure fairness and predictability to U.S. companies seeking to market their technology in a timely fashion.

Fifth, set forth specific penalties for companies that seek to exploit loopholes or ambiguities or circumvent the limits and ensure their enforcement.

I again commend Messrs. Weldon and Dellums for their leadership in fashioning a much improved title 3 for the bill. The suggested changes I've outlined above, and other changes I hope to offer during the course of the bill's consideration in the House, will strike an even better balance in this important policy debate.

JANE HARMAN.

SUPPLEMENTAL VIEWS OF HON. LORETTA SANCHEZ

Many of us when we think of encryption imagine the "ENIGMA" code breaking machines of World War Two or the American Indian "code talkers" that helped us anticipate and defeat Nazi and Imperial Japanese attacks. Those methods were mechanical or human-based, and often depended on simple arithmetical slight of hand to trick the enemy. Today, encryption is complex mathematical algorithms that have become an entirely new branch of mathematics involving intense academic study.

Until recently encryption was limited to governments and large companies through U.S. export limitations and by the limitations of existing hardware and software technologies. All that began to change as the desktop computer became more prevalent and the computing power available to the average user jumped by leaps and bounds every year. When discussing the power of the PC observers of the information technology industry often predict that the computing power of microprocessors would double roughly every 18 months.

Because of this the rapidly developing speed and growth of computers, the age of the "unbreakable code" has long since passed. Manufacturers of encryption technology are engaged in a rapidly accelerating race to develop the newest and strongest code that can withstand attacks from the increasingly powerful computers of the day. And it isn't just big companies and governments that have the technology to break codes. Last January, a graduate student broke a 40-bit code in just three-and-a-half hours, the toughest code form American companies at the time were allowed to export.

Today, American companies are the world leaders in encryption technology, but other companies and nations are catching up. Strong encryption products and knowledge about the science of cryptography is not limited to the United States. A savvy computer user anywhere in the world can with just a few clicks of the mouse find U.S. export-embargoed encryption. Many freelancing code hackers maintain off-shore Internet meeting sites to discuss the newest holes in encryption products.

The proposed export controls which the Administration argues helps to keep strong encryption out of the hands of foreign adversaries will have little or no effect. Strong encryption is available abroad and US companies are being put at a competitive disadvantage in the global marketplace.

With this bleak and seemingly hopeless picture in mind how do we protect ourselves from the threat of rogue nations and other adversaries cloaking their communications from American National Security efforts? The only viable solution is through supporting a robust and aggressively competitive cryptography industry in the United States. We must ensure that the United States continues to maintain the deepest pool of cryptographic experts in the world.

American export limitations will only serve to create a brain drain of these precious resources as leading scientists leave our shores for more lucrative and accommodating surroundings.

All of us care about our national security and no one wants to make it any easier for criminals and terrorists to commit criminal acts. But we must also recognize encryption technologies as an increasingly sharp double-edged sword. It can also aid law enforcement and protect national security by limiting the threat of industrial espionage and foreign spying, but only when Americans are able to produce the sharpest swords and the strongest encryption.

I would also like to state for the record that for the reasons stated above, I do not support the Dellums-Weldon Amendment to H.R. 695, and would have voted against it.

LORETTA SANCHEZ.

○