Order Code IB96039

CRS Issue Brief for Congress

Encryption Technology: Congressional Issues

Updated July 9, 1998

Richard M. Nunno
Science, Technology, and Medicine Division

CONTENTS

Encryption Technology: Congressional Issues

SUMMARY

Fundamentally, the controversy over encryption concerns what access the government should have to encrypted stored computer data or electronic communications (voice and data, wired and wireless) for law enforcement purposes.

Encryption and decryption are methods of using cryptography to protect the confidentiality of data and communications. When encrypted, a message only can be understood by someone with the key to decrypt it. Businesses and consumers want strong encryption products to protect their information, while the Clinton Administration wants to ensure the law enforcement community's ability to monitor undesirable activity in the digital age.

The Administration's policy promotes the use of strong encryption, here and abroad, as long as it is designed with "key recovery" features where a "key recovery agent" holds a "spare key" to decrypt the information. The Administration would require key recovery agents to make the decryption key available to duly authorized federal and state government entities. Privacy advocates worry that law enforcement entities would have too much access to private information.

The Administration has been using the export control process to influence whether companies develop key recovery encryption products by making it easy to export products with key recovery, and difficult for those products without. Today there are no limits on domestic use or import of any type of encryption, so the Administration has tried to influence what is available for domestic use through export controls since most companies do not want to create two products—one for U.S. use and another for export. U.S. companies believe U.S. export policies hurt their market share while helping foreign companies that are not subject to export restrictions. Many businesses and consumer groups agree that key recovery is desirable when keys are lost, stolen, or corrupted, but want market forces—not government directives—to drive the development of key recovery encryption products. They also object to government having any role in determining who can hold the keys.

In September 1997, the debate shifted to add the prospect that the domestic use policy could change. On September 3, FBI Director Louis Freeh raised the possibility of requiring encryption products manufactured in or imported into the United States to have key recovery features and opened the possibility that key recovery could be enabled by the manufacturer, not only the user. The Administration insists its policy hasn't changed. On September 11, the House Intelligence Committee marked up H.R. 695 with an amendment similar to Freeh's views. On September 24, the House Commerce Committee rejected a similar amendment.

All parties agree that encryption is essential to the growth of electronic commerce and use of the Internet, but there is little consensus beyond that. Seven bills on encryption or computer security have been introduced in the 105th Congress (H.R. 695, H.R. 1903, H.R. 1964, S. 376, S. 377, S. 909, and S. 2067). Hearings have been held in several House and Senate committees. H.R. 695 has been reported by the five committees to which it was referred. S. 909 was ordered reported on June 19 but the report has not been filed. The House passed H.R. 1903 on September 16.

MOST RECENT DEVELOPMENTS

On May 12, Senator Ashcroft introduced S. 2067, the E-PRIVACY Act. Although the bill is generally viewed as pro-industry and pro-privacy, criticism has been voiced by some electronic privacy groups over provisions that would create a "NET Center"in the Department of Justice to assist law enforcement in keeping pace with encryption technology, and that would make use of encryption to obstruct justice a federal crime. Several meetings took place in June among key Members, Administration officials, and computer industry leaders to discuss this bill and the other encryption legislation.

On July 7, the Administration announced plans to relax export controls for strong encryption software without requiring provisions for key recovery, but only for financial institutions in the 45 countries that have acceptable money laundering laws. The Administration has also announced plans to declassify two security algorithms used in the Clipper chip, an encryption device used for unclassified but sensitive government communications.

BACKGROUND AND ANALYSIS

Encryption, Computers, and Electronic Communications

Encryption and decryption are procedures for applying the science of cryptography to ensure the confidentiality of messages. Technically, the issue discussed here is cryptography policy, but since encryption is the most controversial application of cryptography, it is the term used popularly and herein. (There are other methods of using cryptography to protect confidentiality — steganography and "chaffing and winnowing" — but constraints on the length of this issue brief do not permit discussion of them.)

Encrypting messages so they can be understood only by the intended recipient historically was the province of those protecting military secrets. The burgeoning use of computers and computer networks, including the Internet, now has focused attention on its value to a much broader segment of society. Government agencies seeking to protect data stored in their databases, businesses wanting to guard proprietary data, and consumers expecting electronic mail to be as private as first class mail, all want access to strong encryption products. Other users of electronic communications, for example cellular (wireless) phone users who expect calls to be as private as wireline calls, also are showing increased interest in encryption. While encryption is uncommon for telephone users today, the advent of digital telephone services (particularly Personal Communication Services, PCS, a digital form of cellular telephony) is expected to make encrypted voice and data communications over telephones more common.

Whether hardware- or software-based, an encryption product scrambles a message using mathematical algorithms. A corresponding key is needed to decrypt (unscramble) the message, and the key itself also may be encrypted. The algorithm is a series of digital numbers (bits), and the level of difficulty of breaking the code (its "strength") is usually represented by the number of bits in the key. (There are other factors that affect a key's

strength, but in this debate, bit length is used as a benchmark.) Unencrypted data are referred to as “plaintext.” Encrypted data are “ciphertext.”

The National Institute of Standards and Technology (NIST), in conjunction with industry, developed an encryption standard using a 56-bit key in 1977. Called the Data Encryption Standard (DES), it is widely used today in the United States and abroad, often in an enhanced mode called “3-key triple DES” providing the equivalent of a 112- bit key. NIST is currently working to establish a new, stronger standard than DES referred to as the Advanced Encryption Standard (AES). The need for a stronger standard was underscored in June 1997 when DES was broken (see below).

Encryption products are widely available today, including some that use 128-bit keys or more. Some 128-bit encryption software can be downloaded from the Internet. There are no limits on the strength of encryption products used in the United States, whether acquired here or imported. The only limits are on exports. This indirectly influences what is available domestically, however, since most U.S. companies are reluctant to develop two products, one for the U.S. market and another for export. For many years, reflecting the policies of the past three Administrations, the State Department did not allow general exports of encryption with better than 40-bit keys, except for banking and U.S.-owned subsidiaries (for a list of exceptions, see CRS Report 96-232). In December 1996, the Clinton Administration temporarily and conditionally raised the limit to 56 bits for easily exportable encryption products that do not have key recovery features (see box), and removed bit length limits entirely for products with key recovery. Breaking a message encrypted with a 40-bit key by “brute-force” (trying every possible combination of bits until the correct one is found) is not considered difficult. In January 1997, a Berkeley graduate student broke a 40-bit key in 3.5 hours by linking together 250 computers. It is 2^{16} (65,536) times more difficult to break a 56-bit key than a 40-bit key. In 1997, an ad hoc group accomplished the task over 5 months by linking together thousands of computers. Both achievements were in response to a challenge from a prominent encryption product manufacturer, RSA Data Security. Opponents of encryption controls hope the demonstrated vulnerability of 40- and 56-bit keys will influence the on-going encryption debate.

KEY RECOVERY AND KEY RECOVERY AGENTS

Once called "key escrow," key recovery means that when stored data or electronic communications are encrypted, a third party has a copy of the key needed to decrypt the information. The third party is called a key recovery agent (formerly a key escrow agent). Key recovery is widely regarded as useful in cases where a key is lost, stolen or corrupted. Most parties to the encryption debate agree that market forces will drive the development of key recovery-based encryption products for stored computer data because businesses and individuals will want to be sure they can get copies of keys in an emergency. It is less clear if market demands will drive key recovery systems for electronic communications.

The controversy is over government's attempt to "encourage" the development of key recovery-based products through the export control process, the government's role in determining who can serve as key recovery agents, and the extent to which law enforcement agencies could obtain the key if they suspect undesirable activity (terrorism, child pornography, and drug cartels are often cited as examples).

The limit of 40 bits remains for encryption products that do not incorporate key recovery features and for which companies do not plan to create them. Business and consumer groups consider 40-bit keys inadequate to ensure privacy and security. They oppose export encryption controls, or at least want increasingly higher limits on the bit length, without regard to whether the product includes key recovery features. They object to the government

using the export process to force the development of key recovery encryption products, rather than allowing market forces to prevail, and to the government's role in determining who can serve as key recovery agents. These groups argue that strong encryption is needed, for example, to enhance the prospects for electronic commerce and other uses of computer networks. The willingness of consumers to buy goods via the Internet could be markedly affected by their beliefs as to whether credit card numbers will be secure. Businesses using computers for either internal or external communications need to ensure that competitors or other unauthorized parties cannot gain access to proprietary information. Privacy advocates argue that consumers should be assured that personal, medical and financial information transmitted by or stored in computers will be protected. They note that since 128-bit non-key recovery encryption is available worldwide either by downloading it from the Internet or by buying it from foreign firms, the U.S. government already has lost control of influencing its availability. A September 1997 survey conducted by Trusted Information Systems [www.tis.com/docs/research/crypto/survey] shows 653 foreign encryption products available from 29 countries (in addition to 948 U.S. products). Of the foreign products, 275 employ DES, demonstrating the widespread availability of strong encryption. An April 1998 report by the Economic Strategy Institute, *Finding the Key*, concluded that if the Administration's current policies remain in effect, the U.S. economy will lose $35-96 billion over the next 5 years (1998-2002) in lost encryption product sales; slower growth in encryption-dependent industries; foregone cost savings and efficiency gains from the Internet, intranets, and extranets; and indirect effects throughout the economy.

PROPONENTS AND OPPONENTS OF ENCRYPTION EXPORT CONTROLS

Proponents include the Clinton Administration (notably the Department of Justice and the National Security Agency) and others who are concerned about the ability of terrorists and other criminal groups to conduct activities unmonitored if strong non-key recovery encryption is widely available.

Opponents include:

- computer hardware and software manufacturers who do not want to develop separate products for domestic and foreign markets and worry they will lose market share to foreign competitors who do not have to abide by such limits. They also are concerned that no one may buy encryption products for which the U.S. government can obtain the key.
- U.S. businesses that want to use the same computer systems they have in their home offices with their foreign clients; and
- privacy and consumer groups who want individuals to have access to the best encryption possible without regard to key recovery features.

Supporters of encryption export controls agree that strong encryption is needed but insist that law enforcement and national security concerns demand that, when authorized, the government be able to intercept and decrypt electronic communications or decrypt stored computer data where undesirable activity is suspected. Law enforcement and national security officials want to ensure their ability to access the plaintext of the information. The method most often discussed is to obtain the key needed to unscramble encrypted information from key recovery agents. Hence, they support strong encryption products as long as they include key recovery features. What they want to limit is the development of strong non-key recovery products. While conceding some strong non-key recovery encryption products already are available, they claim use of these products is not widespread. They argue that while the U.S. government cannot prevent the availability of strong non-key recovery encryption, at least it can be restrained, and future generations of encryption products (with key recovery) will displace those now in use.

Although the publicity surrounding the encryption debate so far has centered on access to stored computer data, electronic communications are equally important to the law enforcement and national security communities. An Internet message, for example, is stored data when it resides on a server or an individual's computer, but it is an electronic communication while it is being transmitted between computers. The encryption export regulations apply to products for encrypting other electronic communications, not just those between computers. Telephones, whether wired or wireless (such as cellular phones), are also covered, for example. The 1994 Communications Assistance to Law Enforcement Act (CALEA, often called the "Digital Wiretap" Act, P.L. 103-414) requires telecommunications carriers to ensure their equipment permits the interception of any electronic communication by law enforcement officials. If the communication is encrypted, law enforcement agencies want to ensure they can decrypt it, too. (CALEA requires the telecommunications carrier to provide decrypted information if the carrier itself is responsible for the encryption, but not if the customer has encrypted it.)

Clinton Administration Policy

The Clinton Administration has strongly supported arguments by law enforcement and national security agencies that the government must be able to gain access to the plaintext of encrypted electronic data and messages when undesirable activity is suspected. While there is interest in international criminal activity, the Administration (notably the FBI) also wants to be able to monitor domestic criminal activity. U.S. policy has been to permit use of any strength encryption, without a key recovery requirement, in the United States. Rather than attempting to change that policy directly, the Administration has been using the indirect route of export controls to influence what types of encryption products are available, both here and abroad. However, on September 3, 1997, FBI Director Freeh raised the possibility of imposing domestic use restrictions (see **Senate Judiciary Committee**). Although the Administration insists its policy hasn't changed and Freeh was speaking only for the FBI, his statement is viewed by many as a turning point in the encryption debate.

For many years, the Clinton Administration sought to restrain the development of strong encryption products by not permitting export of better than 40-bit encryption (with a few exceptions). In the fall of 1996, it focused its policy on the need for strong encryption, as long as it includes key recovery features. The key recovery agent would be required to give the key to duly authorized law enforcement officials if undesirable activity is suspected (the three types most often cited are drug cartels, child pornographers, and terrorists).

The Clinton Administration has tried several approaches to promote "voluntary" use of key recovery agents. In April 1993, the Administration released its "Clipper chip" policy requiring emplacement of special encryption computer chips (called Clipper) into new government equipment for voice communications, with two government agencies, NIST and the Department of Treasury, jointly serving as key escrow agents (each holds part of the key). The Administration implemented this policy in 1994 for sensitive but unclassified voice communications in the federal government through a Federal Information Processing Standard (FIPS) called the Escrowed Encryption Standard (EES, or FIPS-185).

The Administration hoped that industry would accept the Clipper chip for its own use on a voluntary basis, but industry strongly objected to the key escrow provisions, particularly the fact that government agencies would hold the keys. In July 1994, the Administration

agreed to work with the private sector to develop a "voluntary" key escrow system for data using "trusted third parties" as escrow agents instead of government agencies. This proposal is sometimes referred to by its detractors as "Clipper II."

Industry continued to object to the key escrow concept as well as the export controls, leading to the legislation discussed below. On May 20, 1996, the Administration released a draft paper on encryption policy, followed by a July 12 statement by Vice President Gore. Called "Clipper III" by its opponents, these documents outlined policy changes the Administration was considering. Among other things, the term "key recovery" replaced "key escrow." The new term emphasizes the positive attributes of key escrow in providing a means to recover a key that is lost, stolen, or corrupted. Furthermore, "key escrow" had come to be identified with the concept of the government holding the key. Under the new policy, a trusted third party (TTP) or an organization itself can serve that function ("self escrow"), with some restrictions.

Current Policy

Vice President Gore formally announced those changes on October 1, 1996. The associated executive order was signed November 15 and released along with a presidential memorandum incorporating additional details of the policy. Under the 1996 policy:

- The lack of restrictions on domestic use or import of any encryption continues;
- There is no algorithm or key length restrictions on the export of encryption products if a key recovery system is in place for that product;
- For products without key recovery systems, 56-bit encryption products can be exported after a one-time review for up to 2 years. By then, the exporter must have developed a key recovery system. The license would be granted in 6-month increments, to hold exporters to a required timetable to ensure the key recovery system is being developed. If key recovery systems are not produced, the export license will not be renewed;
- Trusted parties must serve as key recovery agents, but in some cases, organizations would be allowed to escrow the keys themselves (self-escrow) if they meet certain requirements; and
- Commercial encryption is removed from the Munitions List and responsibility for commercial export licensing is transferred from the State Department to the Commerce Department. The Department of Justice has an advisory role in commercial encryption export decisions.

The White House said that foreign governments could apply to U.S. courts to gain access to keys, as they do now when seeking other types of evidence.

On December 30, 1996, the Administration published an "interim final" regulation, effective that day, transferring primary responsibility for commercial encryption export control from the State Department to the Commerce Department. The Commerce Department expects modifications to this version in response to comments received, although revised regulations have not been released. Among the expected changes are waivers for banking and other financial applications. The relaxed restrictions on 56-bit encryption will end on December 30, 1998, under existing policy. Undersecretary of Commerce William Reinsch

said at an April 24, 1998 meeting of the Congressional Internet Caucus that the government is working with industry to develop a plan on how to proceed after that date.

On March 4, 1998, Vice President Gore wrote to Senator Daschle restating the Administration's desire for a "balanced approach" to encryption policy and seeking a "good faith dialogue" to "produce cooperative solutions, rather than seeking to legislate domestic controls." The letter added that the discussions could also enable additional steps to relax export controls on encryption products. On April 15, Secretary of Commerce Daley made a speech announcing the release of a new report on electronic commerce wherein he said that although the Administration's policy was the right one, its implementation was a failure. He urged both industry and government to strive harder to reach consensus on the issue.

In April 1998, Undersecretary of Commerce Reinsch commented at a Congressional Internet Caucus meeting that the Administration was not currently looking for a legislative solution to the encryption issue. In 1997, however, he had outlined key aspects of proposed legislation that was being drafted within the Administration. A version of the draft legislation was made available on the Web site of a group opposed to export controls, but the Department of Commerce would neither confirm nor deny it was a draft of the bill. Two months later, Mr. Reinsch said that the Administration had decided not to propose legislation at that time. Following FBI Director Louis Freeh's testimony to the Senate Judiciary Committee on September 3, 1997 (see **Senate Judiciary Committee**), the existence of another administration draft bill, dated a week before the hearing, became widely known that reflected Freeh's comments about the need for domestic use restrictions. Mr. Reinsch stated the next day that Freeh's comments reflected the FBI's view, not the Administration's, and did not indicate a change in Administration policy. Vice President Gore stated on September 9 that the Administration was not changing its policy. A spokeswoman for Mr. Gore later said the draft bill was "technical assistance" requested by Congress. On September 11, the House Intelligence Committee approved an amendment to H.R. 695 similar to Freeh's position about the need for key recovery to be built into encryption products.

Industry Reaction

Many participants in this debate agree that market forces will lead to the development of key recovery-based encryption products for stored data because companies and individuals will want to be able to replace lost, stolen or corrupted keys. The debate is over the government's role in "encouraging" the development of key recovery products through export regulations, and the access government wants to the keys. Also of concern is the government's inclusion of other electronic communications.

Many computer companies continue to argue against the Administration's policy, but many also are moving forward in developing key recovery products that satisfy the new policy. A group of companies formed the Key Recovery Alliance [www.kra.org] in 1996 to focus on identifying barriers to the development of marketable key recovery products. KRA has over 60 members, including Hewlett-Packard, IBM, Intel, NEC, RSA, and UPS. In April, 1998, Mr. Reinsch stated that the Department of Commerce had approved about 50 applications that had been submitted together with commitment plans for key recovery. While continuing his strong opposition to the government's encryption policy, James Barksdale, CEO of Netscape, has credited that policy with successfully pushing industry to develop key recovery encryption products.

On March 4, 1998, a group of more than 100 companies and organizations (including some who also are members of the Key Recovery Alliance) formed the Americans for Computer Privacy (ACP) coalition [www.computerprivacy.org]. The group is lobbying in favor of using strong encryption, against export controls on strong encryption, and against mandatory key recovery. Among the members are Netscape, Microsoft, Sybase, the National Rifle Association, the Law Enforcement Alliance of America, and the Business Software Alliance. ACP is widely credited as having been influential in drafting S. 2067.

On another front, Network Associates announced in March 1998 that it had arranged for a Swiss company to develop its own software product using specifications in a book by Philip Zimmerman, the creator of Pretty Good Privacy (PGP). Network Associates bought Mr. Zimmerman's company in 1997. PGP is a 128-bit encryption product that does not incorporate key recovery and hence could not be exported under the current regulations. (An older version is available via the Internet, however, which sparked a multi-year Justice Department investigation of Mr. Zimmerman that resulted in no action against him). Since the book may be exported, and the Swiss company received no technical assistance from Network Associates, the company believes no laws were broken. The Swiss product will be sold by a Dutch firm using the PGP name. Opponents of encryption controls point to this as evidence that the U.S. government cannot control the spread of non-key recovery encryption. The Commerce Department said it would look closely into the arrangement.

NRC Report

In May 1996, the National Research Council (NRC) released a comprehensive report entitled *Cryptography's Role in Securing the Information Society* (the "CRISIS" report). It stressed that national policy should make cryptography broadly available to all legitimate elements of society, promote continued economic growth and leadership of key U.S. industries, and ensure public safety and protection against foreign and domestic threats. Among the recommendations: key escrow is an unproven technology and the government should experiment with it and work with other nations, but not aggressively promote it now; export controls should be relaxed progressively, but not eliminated; and encryption policy issues can be debated adequately in public without relying upon classified information. The report also recommended that no law should bar the manufacture, sale or use of any form of encryption within the United States; and government should promote information security in the private sector. Importantly, the report underscored that utilization of strong encryption and law enforcement objectives can be mutually compatible.

Action in the 105th Congress

Three bills in the House and four in the Senate concerning encryption or related issues have been introduced in the 105th Congress; one has passed the House (H.R. 1903). Three (H.R. 695, S. 376, and S. 377) are versions of bills considered in the 104th Congress and generally favor relaxed encryption export controls (S. 376 also deals with the issue of key recovery agents). Four new bills also have been introduced. The McCain/Kerrey/Hollings bill, S. 909, reflects a philosophy closer to that of the Clinton Administration than the three previous bills. Representative Sensenbrenner's bill (H.R. 1903) focuses broadly on computer security issues and the role of the NIST. Representative Markey's bill (H.R. 1964) focuses

broadly on computer privacy and security issues. Senator Ashcroft's bill is generally viewed as pro-industry and pro-privacy. Hearings have been held by six House committees (Commerce, International Relations, Intelligence, Judiciary, National Security, and Science) and two Senate committees (Judiciary; and Commerce, Science, and Transportation).

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

On February 12, 1997, Representative Goodlatte introduced H.R. 695. Originally referred to the Committees on Judiciary and International Relations, on June 26, it was additionally referred to the Committees on Commerce, National Security, and Intelligence. Several hearings have been held (see **Legislation**). All five committees have completed markup. A summary of the amendments adopted by the various committees, some of which significantly change the character of the original bill, is shown in the following table. The next step is for the Rules Committee to determine which, if any, of these versions will be the vehicle for further action.

H.R. 695

Version	Comments
As introduced February 12	Section 2 defines terms, codifies existing domestic use policy, prohibits mandatory use of key recovery, prohibits requiring anyone in lawful possession of a key to turn that key over to another person except for law enforcement personnel acting under law, and makes it a crime to use encryption in furtherance of crime; Section 3 gives Secretary of Commerce exclusive jurisdiction over export of commercial encryption, and prohibits export controls on "generally available" commercial encryption except for military end-uses or to identified individuals or organization in specific foreign countries.
As reported from House Judiciary May 22 (H.Rept. 105-108 Pt. I)	Adopted amendments (voice) that make technical changes to the definitions; exempt members of intelligence community (as well as law enforcement) from the prohibition against getting encryption key if acting under law; clarify that the new crime of using encryption in the commission of a crime applies only to the use of encryption to avoid detection of some other federal felony and only when it is knowingly and willfully used to avoid detection; and add a fourth section that directs the attorney general to collect data on cases in which encryption has interfered with, impeded, or obstructed the ability of the Justice Department to enforce law.
As reported from House International Relations July 25 (H.Rept. 105-108 Pt. II)	Adopted amendment (unanimous consent) approved by subcommittee that removes the distinction between mass market and customized software; expands section 3 to include consumer products that do not necessarily fall under the umbrella of "computing" products; broadens the scope and definition of "generally available" to include hardware with encryption capabilities; and adds a fourth section regarding international cooperation. Defeated a Gilman amendment (13-22) that would have allowed the President to deny export licenses for national security reasons (including "the ability of law enforcement agencies ... to combat espionage, terrorism, illicit drugs, kidnapping, or other criminal acts, or otherwise would involve the potential for loss of human life.").

Version	Comments
As reported from House National Security Sept. 12 (H.Rept. 105-108 Pt. III)	Adopted amendment (45-1) replacing Section 3 (export controls) with new section that gives the Secretary of Commerce, with the concurrence of the Secretary of Defense, responsibility for export of encryption not controlled through the Munitions List, provides that encryption products may be exported following a one-time review if they do not exceed the level specified by the President as not harmful to national security, and directs the President to notify Congress within 30 days of enactment and annually thereafter on the maximum level of encryption that can be exported without harming national security.
As reported from House Intelligence Sept. 16 (H.Rept. 105-108 Pt. IV)	Adopted amendment (voice) requiring exports of encryption products to submit to a one-time review and include features allowing for immediate access to plaintext or to decryption information; requires encryption products manufactured and distributed for sale or use in, or imported for sale or use into, the United States after January 31, 2000 to include features that provide immediate access to plaintext data or decryption information from the encryption provider; allows for use of encryption products currently employed even after January 31, 2000; allows for law enforcement access with delayed notification requirements similar to those allowed in current wiretap statutory provisions; provides civil remedies and criminal penalties for unlawful access to or disclosure of plaintext or decryption information; and requires U.S. government procurement of encryption technology that includes features allowing for immediate access to plaintext or decryption information. The amendment does not change law enforcement's statutory requirements prior to intercepting oral, wire, or electronic communications, or stored data (law enforcement must have separate court order to have the data, including communications, decrypted).
As reported from House Commerce Sept. 29 (H.Rept. 105-108 Pt. V).	Adopted Tauzin amendment (voice), as amended by the Markey-White amendment (40-11), that modifies section 2 by adding creation of a National Electronics Technologies Center in the Department of Justice to help law enforcement keep pace with encryption technology; prohibits conditioning laws or regulations governing issuance of certificates of authentication or authority on a requirement to escrow or otherwise share private keys, or conditioning licensing, labeling, or other regulatory scheme for any encryption product on a requirement for key escrow; requires an NTIA study on the implications of mandatory key recovery; increases penalties and modifies language concerning use of encryption in furtherance of a crime; and provides liability protection for those providing plaintext to law enforcement or government entities pursuant to judicial process. Defeated Oxley-Manton amendment (16-35) that would have, inter alia, imposed domestic use restrictions.

S. 376: Encrypted Communications Privacy Act (ECPA)

On February 27, 1997, Senator Leahy introduced S. 376, the Encrypted Communication Privacy Act of 1997. S. 376 would prohibit mandatory use of key recovery but allow law enforcement to access the key under court order if key recovery is used; codify existing

domestic use policy; give the Secretary of Commerce exclusive jurisdiction over commercial encryption exports; liberalize export controls; make it a crime to use encryption to obstruct justice; and establish liability protection and penalties for "key holders." The bill also establishes procedures for foreign governments to access keys or decryption assistance. The Senate Judiciary Committee held a hearing on key recovery on July 9, 1997.

S. 377: Promotion of Commerce On-Line in the Digital Era (PRO-CODE)

Also on February 27, 1997, Senator Burns introduced S. 377, the PRO-CODE Act of 1997. The bill prohibits mandatory key recovery and establishes an Information Security Board as a forum to foster communication and coordination between industry and government. The bill codifies existing domestic use policy and gives the Secretary of Commerce exclusive jurisdiction over commercial encryption exports. It liberalizes export controls but requires the publisher or manufacturer of encryption software or hardware to report to the Secretary of Commerce within 30 days after exporting a product on the product's encryption capabilities. The report would include the same information required under the December 30, 1996 regulations, but would be provided after export instead of as a condition of obtaining a license. The Senate Commerce, Science and Transportation Committee held a hearing on the Burns bill on March 19. As discussed below, Senator Burns offered a version of S. 377 as an amendment to S. 909 during markup of the latter bill, but the amendment failed 8-12.

S. 909: The Secure Public Networks Act

On June 16, 1997, Senators McCain, Kerrey, and Hollings introduced S. 909, the Secure Public Networks Act. The bill was referred to the Senate Commerce, Science, and Transportation Committee, which ordered it reported, amended, on June 19. The report has not been filed, however. No hearings were held. Briefly, the bill codifies existing domestic use policy; establishes penalties for use of encryption in commission of a crime; encourages but does not require use of key recovery; establishes procedures for government approval of key recovery agents and certificate authorities; requires key recovery agents, whether or not registered by the government, to disclose recovery information to lawfully authorized federal or state government entities; provides liability protection for key recovery agents acting pursuant to the Act; requires that encryption products procured by the U.S. government or purchased with federal funds for use in secure networks be based on a "qualified system of key recovery", and that future encrypted communications networks established by the government or with the use of federal funds use qualified systems of key recovery; permits export of 56-bit encryption products without key recovery if they meet certain conditions, and directs the President to annually review that limit and increase it for products where similar products are widely available for export from other nations; permits export of any strength encryption product if it is based on a qualified key recovery system and meets certain other conditions; establishes an Information Security Board to make recommendations to the President and Congress on a variety of issues; and allows the President to waive provisions of the bill for national security or domestic safety and security reasons. During markup, the committee adopted a Kerry (MA) amendment establishing an Encryption Export Advisory Board (EEAB) with four government (CIA, FBI, NSA and the White House) and four industry representatives to make recommendations on whether export exemptions should be granted for non-key recovery products stronger than 56-bits. Several other amendments also

were adopted. Senator Burns offered a version of his bill, S. 377, as an amendment to S. 909, but it was defeated 8-12.

On March 4, 1998, Senators McCain and Kerrey issued a press release announcing modifications to the bill: the EEAB would be composed of eight industry and four government representatives (instead of four from each) who would "approve levels of encryption for export based on worldwide availability or anticipatory availability"; the President could still veto the Board's decisions for national security reasons, with notification to Congress required; U.S. companies could export products with optional recovery features to approved end users; use of key recovery remains optional in the United States, but when it is used, the key could "only be obtained by the government by a court order subpoena" as opposed to several other legal means in the original bill; and dual registration of certificate authorities and key recovery agents was eliminated.

Senate Judiciary Committee Hearings

The Senate Judiciary Committee has requested sequential referral of S. 909 and held a hearing on July 9, 1997 on key recovery issues that included discussion of that bill. Senator Kerrey testified that he was willing to modify S. 909 to meet some objections. FBI Director Louis Freeh expressed reservations about the bill because it allows widespread use of strong encryption within the United States regardless of whether it has key recovery. Director Freeh amplified his concerns at a September 3 hearing before the Subcommittee on Technology, Terrorism, and Government Information. He stated that he wants U.S. manufacturers to be required to build key recovery into encryption products, and that imported encryption products also be required to include key recovery. He further stated that there were different methods for achieving the goal of immediate lawful decryption: "That could be done in a mandatory manner. It could be done in an involuntary manner. ..." He later added that he thought legislation should first include the requirement that key recovery be built into encryption products and "then take up the more complex discussion about how that's enabled...." He also stated that Internet Service Providers should be required to have the capability to decrypt communications immediately. He stressed that the FBI was not asking for any new authorities, that it is a matter of technically being able to do tomorrow what they can do today in terms of monitoring criminals and terrorists. At a hearing the next day before the House Commerce Committee, Undersecretary of Commerce Reinsch stated that Director Freeh was speaking for the FBI and not the Administration (see **Clinton Administration Policy: Current Policy**). On March 17, 1998, the Subcommittee on Constitution, Federalism, and Property Rights held another encryption hearing (see **S. 2067**, below).

S. 2067: Encryption Protects the Rights of Individuals from Violation and Abuse in Cyberspace (E-PRIVACY) Act

Senator Ashcroft et al. introduced S. 2067, the E-PRIVACY Act, on May 12, 1998. The bill was referred to the Senate Judiciary Committee. Senator Ashcroft's Subcommittee on Constitution, Federalism, and Property Rights had held a hearing on the issue on March 17, 1998, that primarily addressed the constitutionality of requiring the use of key recovery. S. 2067 prohibits mandatory key recovery and codifies existing domestic use policy. The bill prohibits federal or state agencies from linking the use of encryption for authentication or identification to the use of encryption for confidentiality purposes; requires that the use of

encryption products be voluntary and market-driven; and authorizes government agencies to purchase encryption products, but such products that use key recovery must be interoperable with commercial encryption products. Procedures are set forth for U.S. and foreign law enforcement agencies to access decryption keys or assistance in decrypting electronic communications or stored data. Included is establishment of a National Electronic Technologies Center (NET Center) to help law enforcement keep pace with encryption technology. Use of encryption to obstruct justice would be a crime. The bill gives the Secretary of Commerce exclusive control over commercial encryption product exports; allows export of generally available encryption products after a one-time review except for products designed or modified for military use; permits unrestricted export of customized encryption hardware and software products if a comparable product is or will be available within 18 months from foreign sources; establishes an Encryption Export Advisory Board to determine whether comparable foreign products are commercially available; prohibits restrictions on encryption exports for non-confidentiality purposes; and provides that nothing in the Act limits the President's authority to prohibit export of encryption products to countries that support international terrorism or to impose embargoes on exports to or imports from a specific country. The bill also provides that the contents of electronic records in networked electronic storage be treated in law as though the record had remained in the possession of the person who created the record and that government entities may only access the contents of the record under circumstances specified in the bill. The bill also has provisions regarding the circumstances under which the government may require a mobile electronic communication service to reveal the real-time physical location of a subscriber, and may obtain information from pen register and trap and trace devices.

H.R. 1903: The Computer Security Enhancement Act of 1997

Representative Sensenbrenner introduced the Computer Security Enhancement Act, H.R. 1903, on June 17, 1997. The House Science Committee's Technology Subcommittee held a hearing on June 19, and the bill was reported on September 3 (H.Rept. 105-243). The bill amends and updates the Computer Security Act of 1987, enhancing the role of the National Institute of Standards and Technology (NIST). As passed by the House on September 16, the bill requires NIST to promote the use of commercial-off-the-shelf encryption products by civilian government agencies; clarifies that NIST standards and guidelines are not intended as restrictions on the production or use of encryption by the private sector; provides funding for computer security fellowships at NIST; and requires the National Research Council to conduct a study of public key infrastructures. A section that required NIST to develop standardized tests and procedures to evaluate the strength of foreign encryption products was removed before passage. The bill was referred to the Senate Commerce Committee, which held a computer security hearing on February 10, 1998.

H.R. 1964: Communications Privacy and Consumer Empowerment Act

Representative Markey introduced H.R. 1964 on June 19. The bill covers a range of computer privacy and security issues, and was referred to the Commerce Committee. With regard to encryption, section 203 of the bill would codify existing domestic use policy, prohibit the government (federal or state) from conditioning the issuance of certificates of authentication or certificates of authority upon use of key recovery systems, and prohibit the government (federal or state) from establishing a licensing, labeling or other regulatory scheme that requires key escrow as a condition of licensing or regulatory approval. The bill

also requires the National Telecommunications and Information Administration (NTIA) to conduct a study on, inter alia, how data security issues affect electronic commerce, including identification of generally available technologies for improving data security. Such technologies would include encryption.

Issues

Key Recovery

Key recovery is the fundamental tenet of the Clinton Administration policy. The Administration wants law enforcement access to keys for encrypted data stored by computers, transmitted between computers, or other types of electronic communications. Not only does the Administration view this as critical for U.S. users, but it seeks creation of a global key management infrastructure (KMI) to ensure confidentiality for the growth of global electronic commerce, and monitoring undesirable activity (by terrorists, drug cartels, or child pornographers, for example).

Many opponents of encryption controls agree that key recovery has advantages for recovering a lost, stolen, or corrupted key, but believe market forces will drive the development of a KMI for stored computer data without government involvement. Less likely is a market-driven demand for key recovery products for electronic communications. In any case, opponents of controls insist that the government should have no role in choosing who holds the keys. They fear the government will have unfettered access to private files and communications, though the Clinton Administration stresses that proper legal authorization will be required. Liability protection for proper release of keys, and penalties for improper use or release of keys, is an important aspect of Administration policy.

Questions about technical vulnerabilities that could be introduced if key recovery is incorporated into computer systems were raised in a May 1997 report, *The Risks of Key Recovery, Key Escrow, and Trusted Third Party Encryption,* by an ad hoc group of cryptographers and computer scientists. They concluded that key recovery "introduces a new and vulnerable path to the unauthorized recovery of data" and the "massive deployment of key-recovery-based infrastructures to meet law enforcement's specifications will require significant sacrifices in security and convenience and substantially increased costs...."

The Administration notes that global agreement on the need for key recovery and a global KMI is essential to its policy and has been working with the Organization for Economic Cooperation and Development (OECD) to develop guidelines for a global KMI. On March 27, 1997, the OECD released those guidelines which include 8 principles. Principle 6 states that "national cryptography policies *may* allow lawful access to plaintext, or cryptographic keys, or encrypted data" (emphasis added). Hence, OECD neither endorsed nor rejected the concept of law enforcement access to decryption keys. The European Commission published a communication in October 1997 that noted the need for strong encryption to advance electronic commerce and expressed strong reservations about regulating encryption (by requiring key recovery, for example).

Export Restrictions

Using the export process to influence the type of encryption products that are available in the United States and abroad is one strategy of the Clinton Administration policy. The Administration points to threats to national security and public safety that would arise if criminals and terrorists used encryption that the U.S. government could not decrypt. Administration representatives argue that the National Security Agency (NSA), for example, has been able to thwart criminals and terrorists because NSA intercepted communications in time; if those communications had been encrypted with strong encryption, their task would have been much more difficult. NSA expresses particular concern about passing a law that does not require companies to notify the government of what encryption products are being exported and to whom. Others point to difficulties in stopping future attacks such as that in Oklahoma City in an era when terrorists could use strong encryption.

Opponents of the Administration's policy counter that the United States, through export controls, cannot prevent access to strong non-key recovery encryption by criminals and terrorists because it is already available elsewhere in the world. They further point out that the current policy of no restrictions on domestic use or import of encryption means that domestic threats would not be affected.

The Administration is using the export process to encourage companies to develop products with key recovery features. There are no limits on the strength of encryption products that can be exported if they include key recovery. Opponents of export controls object to the government essentially mandating the use of key recovery, arguing that foreign companies are not bound by such restrictions. They argue that customers who do not want U.S. law enforcement or national security agencies having access to decryption keys will buy encryption products from foreign suppliers. They insist that the U.S. government cannot control the availability of strong non-key recovery encryption products, since they already can be procured from foreign suppliers, or downloaded from the Internet. They assert U.S. policies simply ensure that U.S. companies will lose market share to foreign competitors and will not achieve the overall objective of assuring law enforcement access to encrypted information of criminal groups. They point out that drug cartels, for example, could develop their own encryption products rather than buying commercially available products that would allow governments to access the keys.

Proponents of export controls concede that some criminal groups may develop their own encryption, but insist that at some point they will have to interact with mainstream companies (such as banks or airlines). If the mainstream companies are using key recovery-based systems, this would provide an opportunity for law enforcement to access at least some of the groups' activities. They also point out that even though law enforcement agencies have been allowed to tap telephone lines for decades, criminals still use telephones because the infrastructure is already in place, easily used, and less costly than building an alternative system for their own use. As for foreign competition, proponents argue that although some strong non-key recovery products are available from the Internet or foreign suppliers, they are not widely used and some are not as strong as their advertisements claim.

Some cases involving encryption export controls have been the basis for legal action. One involves University of Illinois Professor Daniel Bernstein and his attempts to publish, both in print and on the Internet, the source code for his Snuffle encryption algorithm. The

government argued that the export required a license under the Arms Export Control Act (AECA) and the International Traffic in Arms Regulations (ITAR) through which AECA is implemented. On April 15, 1996, U.S. District Judge Marilyn Patel ruled that computer source code is "speech" and protected under the Constitution. On December 18, she further ruled that ITAR represents an unconstitutional prior restraint on free speech. Following the December 30, 1996 shift in jurisdiction over commercial export products from the State Department to the Commerce Department, Bernstein's lawyers asked her to review the new regulations, too. On August 25, 1997 she ruled that the new regulations also violate the First Amendment. The government has appealed the ruling. Arguments were heard December 8, 1997. An opposite ruling was made in March 1996 by Judge Charles Richey in a case involving Philip Karn. Mr. Karn was denied permission to export source code on diskette even though the source code had been published in a book and hence was in the public domain. The State Department designated the diskette as a "defense article" under AECA and denied its export. Judge Richey dismissed the complaint because the AECA does not permit judicial review of what is designated by the President as a "defense article." Mr. Karn appealed the ruling, but by the time the appeal was heard in January 1997, the export regulations had changed so the case was remanded back to DC District Court.

Domestic Use

The focus of the encryption debate shifted in September 1997 to include potential changes to domestic use policy. Current U.S. policy allows any type of encryption to be used in or imported into the United States. Administration concerns that attempting to change this policy would be unsuccessful was a factor in its choice of using export controls to influence what encryption products are available for domestic use. FBI Director Freeh's testimony to the Senate Judiciary Committee on September 3 (described above) heralded a shift in the debate towards the possibility of requiring that key recovery be built into products manufactured in or imported into the United States, and possibly enabled by the manufacturer, not only the user. The Administration asserts that its policy has not changed. Language similar to that enunciated by Director Freeh was included in the House Intelligence Committee's action on H.R. 695. An Oxley-Manton amendment to the bill that would have, inter alia, imposed domestic use restrictions was defeated (16-35) during markup by the House Commerce Committee.

LEGISLATION

H.R. 695 (Goodlatte, et al.)

Safety and Freedom through Encryption (SAFE) Act. Introduced February 12, 1997; referred to Committees on Judiciary and International Relations. On June 26, also referred to Committees on Commerce, National Security, and Intelligence. Hearings held March 20 by Judiciary; May 8 by International Relations; July 30 by National Security; September 4 by Commerce; and September 9 by Intelligence. Reported from Judiciary Committee May 22 (H.Rept. 105-108 Part I); from International Relations Committee July 25 (H.Rept. 105-108 Part II); from National Security Committee September 12 (H.Rept. 105-108 Part III); from Intelligence Committee September 16 (H.Rept. 105-108 Part IV); and from Commerce Committee September 29 (H.Rept. 105-108 Part V).

H.R. 1903 (Sensenbrenner et al.)

Computer Security Enhancement Act. Introduced June 17, 1997; referred to Committee on Science. Hearing by Subcommittee on Technology held June 19. Reported from Science Committee September 3 (H.Rept. 105-243). Passed House under suspension September 16 after section 7 was removed.

H.R. 1964 (Markey)

Communications Privacy and Consumer Empowerment Act. Introduced June 19, 1997; referred to Committee on Commerce.

S. 376 (Leahy, et al.)

Encrypted Communications Privacy Act of 1997. Introduced February 27, 1997; referred to Committee on Judiciary. Hearing on key recovery held July 9.

S. 377 (Burns, et al.)

Promotion of Commerce On-Line in the Digital Era (PRO-CODE) Act of 1997. Introduced February 27, 1997; referred to Committee on Commerce, Science, and Transportation. Hearing held March 19.

S. 909 (McCain, et al.)

Secure Public Networks Act. Introduced June 16, 1997; ordered reported from Commerce, Science and Transportation Committee June 19.

S. 2067 (Ashcroft, et al.)

Encryption Protects the Rights of Individuals from Violation and Abuse in CYberspace (E-PRIVACY). Introduced May 12, 1998; referred to Committee on Judiciary. Hearing on topic held March 17, 1998.