Encryption:

Impact on Law Enforcement

March 26, 1999

Laboratory Division
Engineering Research Facility
Quantico, Virginia

For Policy Information:
Digital Telephony & Encryption Policy Unit
Office of Public & Congressional Affairs Section
935 Pennsylvania Avenue, N.W.
Washington, D.C. 20535
(202) 324-5355

For Technical Information:
Signal Analysis & Processing Unit
Electronic Surveillance Technology

Engineering Research Facility
Quantico, VA 22135
(703) 630-6378

EXECUTIVE SUMMARY

Encryption is extremely beneficial when used legitimately to protect commercially sensitive information and communications. The law enforcement community, both domestically and abroad, is extremely concerned about the serious threat posed by the proliferation and use of robust encryption products that do not allow for the immediate, lawful access to the "plaintext" of encrypted, criminally-related communications and electronically stored data in accordance with strict legal requirements and procedures.

The potential use of such commercially-available encryption products by a vast array of criminals and terrorists to conceal their criminal communications and information poses an extremely serious threat to public safety and national security. Law enforcement fully supports a balanced encryption policy that satisfies both the commercial needs of industry for robust encryption while at the same time satisfying law enforcement's public safety and national security needs. Robust, commercially-available encryption products, which include some type of recoverable capability that allows for immediate, lawful access to "plaintext" is clearly the best method to achieve the goals of both industry and law enforcement.

Since April of 1993, the Clinton Administration has expressed support for the adoption of a balanced encryption policy. The Clinton Administration continues to favor a **voluntary** approach to address law enforcement's public safety concerns regarding this issue. The Administration has been attempting to work with industry, through "good faith dialogue," and by allowing "market forces," influence and inducements (mainly changes to existing export regulations) to bring about the development, sale and use of recoverable encryption products.

During the 105th Congress, several encryption-related bills were introduced; however, none were enacted. The main focus of these bills was the relaxation of existing export controls on encryption in an attempt to place U.S. industry in a more competitive position aboard, regardless of the impact on national security and foreign policy. These bills included: **H.R.695**, introduced by Congressman Goodlatte; **S.376**, introduced by Senator Leahy; **S.377**, introduced by Senator Burns; **S.909**, introduced by Senators McCain, Kerrey and Hollings; and **S.2067,** introduced by Senators Ashcroft and Leahy. Of these bills, **only the House Permanent Select Committee on Intelligence's substitute bill to H.R.695 adopted by the Committee during their 9/11/97 mark-up** would have effectively addresses all of law enforcement's public safety concerns regarding commercially-available encryption products manufactured for use in the U.S. as well as the national

security and foreign policy concerns regarding encryption products for export. On February 25, 1999, Congressman Goodlatte re-introduced his encryption export relaxation bill in the 106th Congress **(H.R.850).**

THE PROLIFERATION OF SECURE OR ENCRYPTED COMMUNICATIONS AND ELECTRONICALLY STORED INFORMATION WILL MAKE IT INCREASINGLY DIFFICULT FOR LAW ENFORCEMENT TO OBTAIN AND DECIPHER THE ENCRYPTED CONTENT OF LAWFULLY INTERCEPTED COMMUNICATIONS AND LAWFULLY OBTAINED ELECTRONICALLY STORED INFORMATION THAT IS NECESSARY TO PROVIDE FOR EFFECTIVE LAW ENFORCEMENT, PUBLIC SAFETY, AND NATIONAL SECURITY.

WHAT IS ENCRYPTION?

Encryption is the method of hiding the content of a message. In broad terms, any system or technique that renders a message unintelligible by anyone other than the intended recipient of the message is utilizing encryption. A message which has not been encrypted is often referred to as “plaintext”. After a message has been encrypted, it is referred to as “ciphertext”. Whereas encryption is used to secure a message, decryption is the method for converting ciphertext back to its original plaintext.

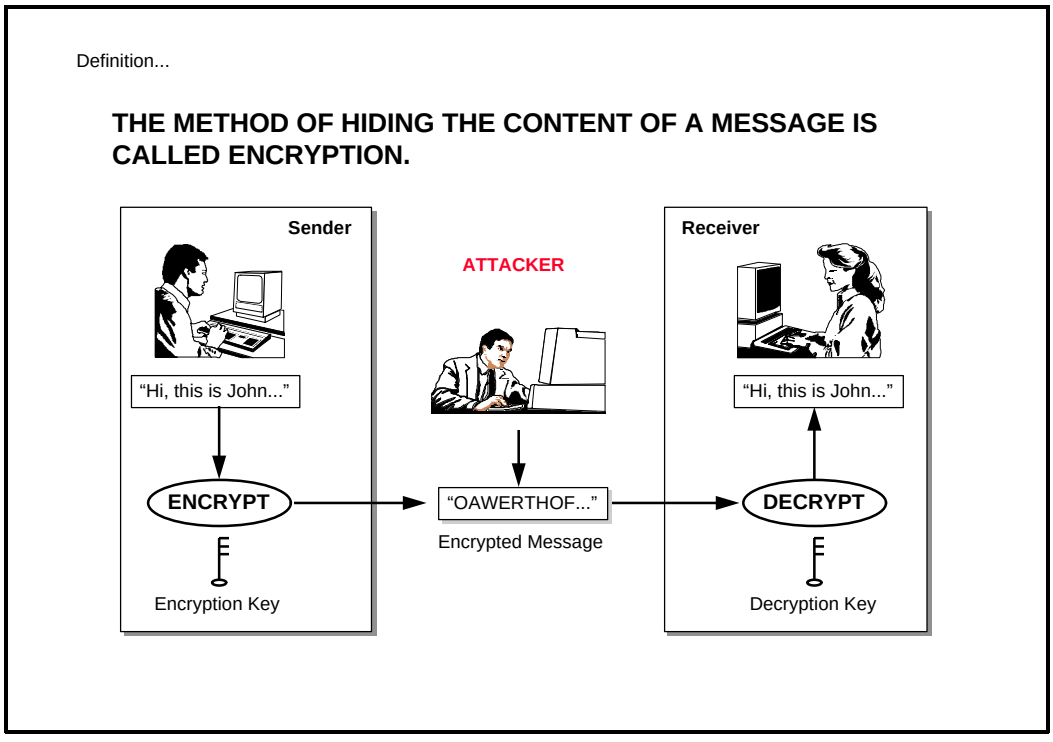
Many encryption systems use a mathematical function, known as a cryptographic algorithm, to encrypt and decrypt messages. Just as a lock box requires a key to lock or unlock it, a cryptographic algorithm requires a key to encrypt and decrypt a

message.

USES AND BENEFITS OF ENCRYPTION

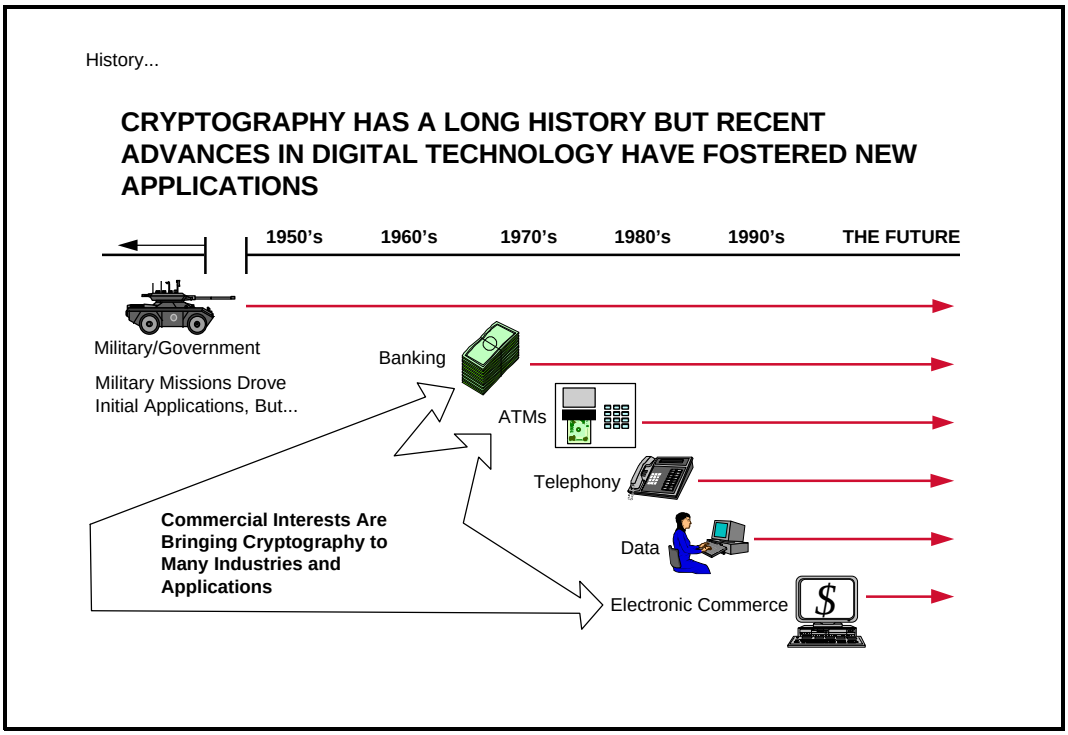
Governments have always been very concerned with the secrecy of information related to military, economic and foreign policy issues. For many years, military and government missions drove the development and use of applications for encryption. Protecting one's intentions from an opposing party is critical and for that reason information security is very important.

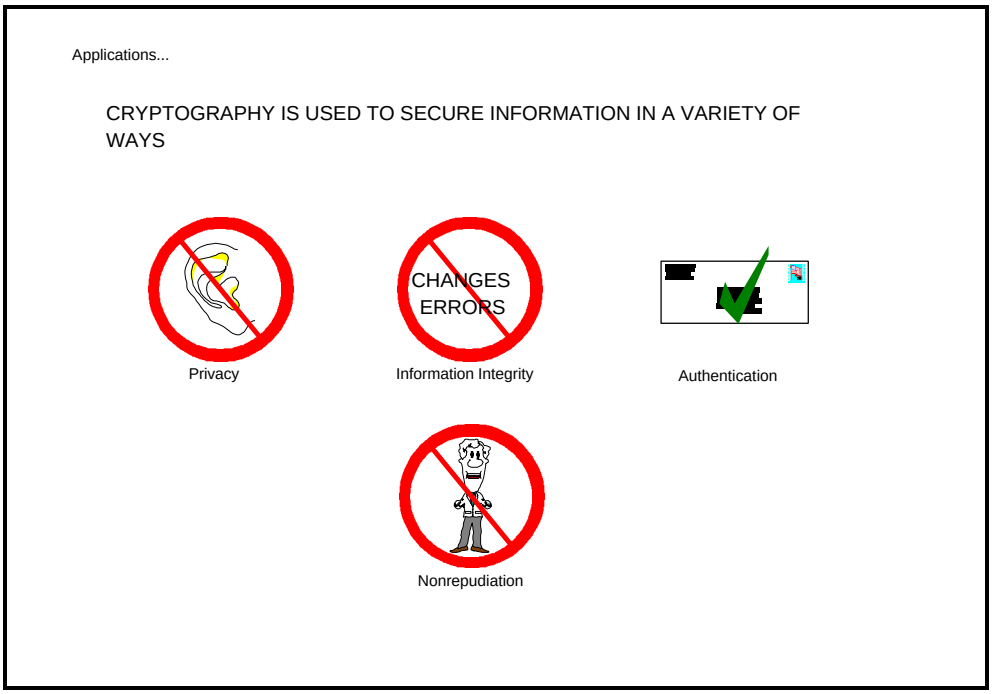
Although encryption software and hardware devices have been commercially available for years, their cost, degradation of voice quality, and user “friendliness” have, in the past made these devices unattractive to the general public. The introduction of digitally-based technologies as well as the widespread use of computers and computer networks which may incorporate privacy features/capabilities through the use of encryption are facilitating the development, production, and use of affordable and robust commercially-available encryption products and services for use by the general public. These encryption systems provide robust security for conventional and cellular telephone conversations, facsimile transmissions, local



and wide area networks, communications transmitted over the Internet (E-mail, etc.), personal computers, wireless

communications systems, electronically stored information, remote keyless entry systems, advanced messaging systems, and radio frequency communications systems.





Various applications will use encryption to provide privacy, information integrity, authentication and non-repudiation. Privacy, or confidentiality, is probably the best known application of encryption. Unauthorized individuals are prevented from listening in or viewing electronic information. Information integrity protects against unauthorized changes to information after it is sent. This is important for the validation of legal electronic documents. Authentication techniques verify the identity of a sender of a message. This provides assurance that the claimed sender (e.g., return address on a letter envelope) of information is the actual sender and vice versa for destination authentication. Non-repudiation ensures that a sender is not able to deny that he or she sent a particular message. This verification is important when auditing or when litigation is being considered.

ADVERSE IMPACTS OF ENCRYPTION

The ability of encryption to ensure the confidentiality and the content of important messages, files or communications of corporations and private citizens can also prevent those same entities from gaining plaintext access to that critical information should the keys needed for decryption become lost or corrupted. Unless there is an alternative plaintext access method, such as a recovery feature incorporated in the encryption product to allow such plaintext access, this important information could be lost forever.

The use of encryption can effectively prevent plaintext access not only to law enforcement acting under proper legal authority, but also to corporations in situations where an employee could potentially use encryption to commit illegal acts, including acts against the corporation. A report from Congress’s Office of Technology Assessment entitled, “Information Security and Privacy in Network Environments,” cited the following: "There is also growing recognition of the potential misuses of encryption, such as by disgruntled employees as a means to sabotage an employer's database."

Encryption can also be used to conceal criminal activity and thwart law enforcement efforts to collect critical evidence needed to prevent, solve and prosecute serious and often violent criminal activities, including illegal drug trafficking, organized crime, child pornography and terrorism. In these instances, the use of encryption to secure the content or confidentiality of information poses substantial threats to law enforcement's abilities to: 1) interpret and analyze stored electronic records and files which have been obtained through court-order or other lawful procedures; and 2) perform court-

ordered electronic surveillance. Encrypted information obtained through the use of lawfully intercepted communications and/or lawfully accessed electronic records or files will be useless in solving crimes and preventing criminal activity unless law enforcement, pursuant to a court order, has immediate access to the plaintext of such encrypted, criminally-related communications and electronically stored data.

As previously discussed, encryption technology was historically used by governments and the military, but legitimate commercial interests and needs are now making this technology increasingly available to industry and individuals alike. As with cellular telephones and other emerging technologies, criminals quickly incorporate readily available technology in furtherance of their illegal activities. A 1993 survey conducted as part of a National Institute of Justice report entitled, “A Summary of a Counternarcotics Technology Needs Assessment of State and Local Law Enforcement Agencies,” revealed that "encryption, scrambling, or other audio countermeasures have been encountered by 28.4% of the respondents, with an additional 23.9% anticipating the use of these countermeasures."

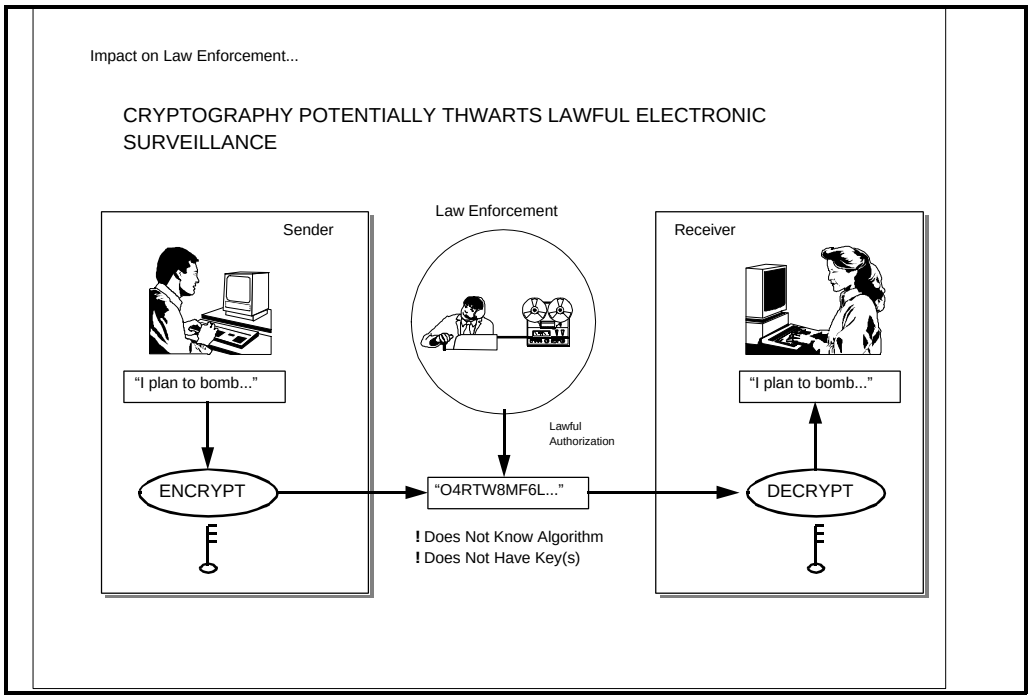
Law enforcement is already beginning to encounter the harmful effects of conventional encryption in some of its most important cases. These include:

> The Aldrich Ames spy case where Ames was told by his Soviet handlers to encrypt computer file information to be passed to them.
>
> The Ramzi Yousef (mastermind of the World Trade Center)/Manilla Air terrorist case where Yousef and other international terrorists were plotting to blow up 11 U.S. owned airliners in the Far East. Data regarding this terrorist plan was found in encrypted computer files discovered in Manilla after Yousef’s arrest.
>
> A child pornography case where the subject’s used commercially-available encryption to encrypt pornographic images of children that were transmitted to other subject’s of the investigation.

The FBI Laboratory Division's Computer Analysis and Response Team (CART) has been tasked with the responsibility of providing assistance in law enforcement investigations where computer generated or stored magnetic media has been obtained pursuant to search and seizure. The CART has seen the number of cases utilizing encryption and/or password protection increase from two percent to at least seven percent, to include the use of 56-bit Data Encryption Standard and 128-bit Pretty Good Privacy encryption over the past two years. Additionally, a recent survey of FBI field offices determined that approximately 40% of the FBI field offices polled had encountered encryption in their investigative efforts to lawfully collect evidence.

THE CONCEPT OF RECOVERABLE ENCRYPTION

Technical solutions that provide robust encryption, combined with some type of recoverable feature which allows for the immediate, lawful access to plaintext of encrypted, criminally-related communications and electronically stored data, is clearly the best way to achieve the goals of both industry and law enforcement. Law enforcement's needs in dealing with its responsibility for protecting public safety and national security are best met by ensuring that commercially-available encryption products manufactured or imported into the U.S. include some type of capability that allows for the immediate access to the plaintext of encrypted, criminal-related data (both transmitted and stored), pursuant to lawful authority (court order).



The concept of recoverable encryption:

Provides a means for corporations to address the misuse of encryption by disgruntled employees;

Ensures the integrity of the investigation through the obtainment of the recovery information or plaintext from a trusted third party (this would also provide the assurance to commercial and individual users of encryption that their encrypted communications and electronically stored information are secure against unauthorized disclosure and illegal"hacker-type" attacks);

Allows for an overt process for legally obtaining recovery information or plaintext that is subject to public scrutiny and accountability;

Provides confidentiality of law enforcement's request for recovery information or plaintext access;

Provides an immediate decryption capability which is available to law enforcement upon presentation of proper legal authority (to include the state and local levels) of encrypted, criminally-related communications or electronically stored information.

Law enforcement’s public safety needs can either be achieved through a voluntary approach, should their be a willingness on the part of industry as a whole (inclusive of all domestic manufacturers and all importers of foreign made products into the U.S.) to effectively address law enforcement’s needs voluntarily; or through a legislative approach, should there be the will on the part of public policy makers to address the issue legislatively; or through a combination of both. Failure to effectively address law enforcement’s needs in this area will ultimately have a devastating adverse impact on the safety and security of the American public.

CLINTON ADMINISTRATION’S POSITION ON ENCRYPTION

Since April of 1993, the Clinton Administration has expressed support for the adoption of a balanced encryption policy that meets the commercial needs of industry for robust encryption while at the same time meeting the public safety needs of law enforcement. Administration representative have been attempting to working with representative of industry to encourage the **voluntary** development, sale, and use of recoverable encryption products within the U.S. The Clinton Administration has steadfastly opposed any legislative effort to impose domestic

controls on encryption, favoring a voluntary approach to address law enforcement's public safety needs through the use of "good faith dialogue," "market-forces," influence and inducements (mainly regulatory change to exiting export controls on encryption products). Law enforcement remains optimistic that such a voluntary approach will be successful in addressing its public safety needs; however, this approach's ultimate success remains uncertain at this time.

On March 4, 1998, the Vice President announced a new Administration initiative to try and bring about the voluntary development of technical solutions that address law enforcement's public safety needs by calling for "good faith dealogue" between industry and law enforcement rather than seeking to legislate domestic controls at that time. Such "good faith dialogue" efforts remain ongoing. Additionally and of significance to law enforcement, on September 16, 1998, the Clinton Administration formally express support for the creation of a centralized law enforcement resource within the FBI to provide law enforcement with urgently needed technical capablities to fulfill its investigative responsibilities in light of the ever increasing proliferation and use of strong, commercailly-available encryption products within the U.S.

Conversely, the Clinton Administration has steadfastly opposed any legislative effort to relax existing export controls on encryption. Such encryption export controls have existed for years to protect national security and foreign policy interest.

ENCRYPTION LEGISLATION

ENCRYPTION-RELATED BILLS INTRODUCED DURING THE 106TH CONGRESS:

H.R. 850, the "**Security and Freedom Through Encryption (SAFE)Act**," introduced by Congressman Goodlatte (R-6th-VA) on February 25, 1999.

H.R. 850 is almost identical to the bill Congressman Goodlatte introduced during the 105th Congress(H.R. 695). H.R. 850 would largely remove existing export controls on hardware and software encryption products of comparable strength to those that are commercially available from a foreign supplier, regardless of the adverse impact to national security. The bill would also place a prohibition on mandatory key recovery encryption by the government and includes a provision making it a crime to use encryption in furtherance of a criminal act.

The following is an overview of the bill's progress during the 106th Congress:

* **H.R. 850** - On March 4, 1999, the House Judiciary Committee's Subcommittee on Courts and Intellectual Property held a hearing concerning the bill with witnesses from NSA, the Justice Department and the Commerce Department testifying in opposition to the bill. On March 11, 1999, despite the aforementioned testimony, the Subcommittee held a mark-up concerning the bill and favorable reported the bill out of Subcommittee (Congressman Goodlatte is a member of that Subcommittee).

On March 24, 1999, the full House Judiciary Committee held a mark-up concerning H.R. 850 and, by a voice vote, favorably reported the bill out of committee without amendments. During the mark-up Congressman McCollum (R-8th-FL) expressed concerns about the bill's adverse impact on law enforcement, national security and intelligence interest, should encryption products that do not allow for immediate plaintext access proliferate within the U.S. and aboard. Congressman McCollum then offered an amendment to the bill's export provisions that would require all hardware and software encryption products for export to include features that allow for immediate plaintext access capabilities for use when there is lawful authorization to obtain such plaintext. Congressman Goodlatte immediately raised a point of order objection, asserting that the amendment was not germane and, without debate, Chairman Hyde ruled that Congressman McCollum's amendment did not fail under the jurisdiction of the Judiciary Committee. It is anticipated that the bill will be referred to the House International Relations, Armed Services, Intelligence and Commerce Committees for consideration.

ENCRYPTION-RELATED BILLS INTRODUCED DURING THE 105TH CONGRESS:

H.R. 695, the "**Security and Freedom Through Encryption (SAFE) Act**," introduced by Congressman Goodlatte (R-6th-VA) on February 12, 1997;

S. 376, the "**Encryption Communications Privacy Act of 1997**," introduced by Senator Leahy (D-VT) on February 27, 1997;

S. 377, the "**Promotion of Commerce On-Line in the Digital Era (Pro-CODE) Act of 1997**," introduced by Senator Burns (R-MT) on February 27, 1997;

S. 909, the "**Secure Public Networks Act**," introduced by Senators McCain (R-AZ), Kerrey (D-NE), Hollings (D-SC) on June 16, 1997.

S. 2067, the "**Encryption Protects the Rights of Individuals from Violation and Abuse in Cyberspace (E-Privacy) Act,"**

introduced by Senators Ashcroft (R-MO) and Leahy (D-VT) on May 12, 1998.

*** NONE OF THE AFOREMENTIONED ENCRYPTION BILLS WERE ENACTED DURING THE 105TH CONGRESS.** Four of the aforementioned encryption-related bills [Goodlatte (H.R. 695), Leahy (S. 376), Burns (S. 377), and Ashcroft/Leahy (S. 2067)] would have largely remove existing export controls on hardware and software encryption products of comparable strength to those that were commercially available from a foreign supplier, regardless of the adverse impact to national security. All five bills would have placed a prohibition on mandatory key recovery encryption by the government and included provisions making it a crime to use encryption in furtherance of a criminal act. The McCain/Kerrey, Leahy, and Ashcroft/Leahy bills would have allowed for the voluntary use of key recovery encryption and would have established in law requirements for the release of decryption keys to law enforcement (Leahy and Ashcroft/Leahy bills by court order, McCain/Kerrey bill by subpoena).

The following is an overview of each to the aforementioned bills' progress during the 105th Congress:

*** H.R. 695** - Reported favorably out of the House Judiciary Committee on May 14, 1997 with three amendments. (Congressman McCollum's amendment--members of the Intelligence Community could obtain key recovery information if escrowed, Congressman Asa Hutchinson's amendment--AG is to maintain records regarding the number of cases where encryption prevented law enforcement from enforcing the law, and Congressman Delahunt's amendment--would make it a felony to encrypt information of a criminal nature). The bill was then referred to the House International Relations Committee for consideration and appropriate action.

On May 24, 1997, the House International Relations Committee's Subcommittee on International Economic Policy and Trade held a mark-up concerning the bill and favorably reported the bill out of subcommittee by a fourteen (14) to one (1) vote.

On 7/22/97, the House International Relations Committee held a mark-up concerning **H.R. 695**. The Committee voted to report **H.R. 695** out of Committee with no amendments. **H.R. 695** was then referred to the House National Security Committee, the House Permanent Select Committee on Intelligence and the House Commerce Committee for appropriate action.

Hearings were also held concerning **H.R.695** before the House National Security Committee on July 30, 1997, before the House Commerce Committee's Subcommittee on Telecommunications, Trade

and Consumer Protection on September 4, 1997 and before the House Permanent Select committee on Intelligence on September 9, 1997.

The House National Security Committee held a mark-up of **H.R.695** on September 9, 1997 and adopted an amendment which continues to require a "one time review" and export license for export of encryption products. This action effectively addressed the national security concerns associated with the bill.

The House Permanent Select Committee on Intelligence held a mark-up of H.R.695 on September 11, 1997 and adopted an amendment by way of a substitute bill that effectively addressed all of the law enforcement and national security concerns associated with commercially-available encryption products and services manufactured for use in the U.S. as well as for export. Highlights include: requirements for immediate access to plaintext features to be included in all encryption products and services manufactured for use in the United States or imported for use in the United States by 1/31/2000; "one time review" by NSA of all encryption products for export and voluntary enabling of any decryption feature included in encryption products for export by the destination country; provide for criminal and civil penalties for unauthorized access to plaintext or decryption information; and, require the U.S. government to only purchase encryption products which include such immediate access to plaintext features.

On September 24, 1997, the House Commerce Committee held a mark-up of **H.R.695**. Two competing amendments were offered: Congressmen Oxley and Manton offered an amendment to require all encryption products manufactured for use in the U.S. or imported into the U.S. to contain an immediate access to plaintext feature which would have effectively address law enforcement's domestic encryption needs and would be supported by law enforcement; Congressmen Markey and White offered an amendment to establish a "National Electronic Technologies Center" to foster the "exchange of information and expertise" between government and industry. However, the Markey/White amendment provided no funding for this center. It did not mandate industry participation, nor is it the goal of the "Center" to provide law enforcement with immediate decryption technical capabilities. Markey/White was supported by industry but was opposed by law enforcement. The Commerce Committee defeated the Oxley/Manton proposal and adopted the Markey/White Amendment, agreeing to favorably report **H.R.695** out of committee as amended.

H.R.695, as amended by the five committees, was then sent to the House Rules Committee. The Rules Committee, at the discretion of its Chairman, was to consider the different

versions of the bill adopted by the five House Committees (Judiciary, International Relations, National Security, Intelligence and Commerce) to determine if a workable compromise bill could be developed and forwarded to the House floor for action. At the insistence of Chairman Solomon (R-NY-22nd), no action was taken by the Rules Committee concerning H.R. 695 as to ensure that the House did not pass an encryption bill that failed to meet all of the law enforcement and national security needs concerning encryption.

* **S. 909** - Reported favorably out of the Senate Commerce Committee on June 19, 1997 with five amendments: one amendment to section 106 regarding the strength of the subpoena used to obtain recovery information; one amendment to section 201 requiring NIST to release a public reference plan regarding key recovery systems prior to the policy provisions of this section being enforced; one amendment to section 205 to clarify that this section only covers networks for the transaction of government business; and one amendment to section 1005 to define what key recovery means. Another amendment was introduced that would create an export advisory board consisting of a chairman appointed by the President, four (4) industry representatives and four (4) government representatives-one each from the CIA, NSA, FBI and Commerce. The bill was scheduled to be referred to the Senate Judiciary and Intelligence Committees for appropriate action but was never officially reported out of the Senate Commerce Committee.

* **S. 377** - Introduced. Failed to be favorably reported out of the Commerce Committee by a 12 to 8 vote on June 19, 1997 as a substitute to S. 909. Senators Burns, Gorton, Lott, Ashcroft**, Abraham**, Brownback, Dorgan and Wyden voted in favor of S.377; Senators McCain, Stevens, Hutchison, Snowe, Frist, Hollings, Inouye, Ford, Rockefeller, Kerry, Breaux and Bryan voted against S.377. (** **denotes member of Senate Judiciary Committee**)

* **S. 376** - Only introduced.
* **S. 2067** - Only introduced.