Statement
of

Louis J. Freeh
Director

Federal Bureau of Investigation

on

July 25, 1996

Before the

Committee on Commerce, Science, and Transportation
United States Senate

Regarding

Impact of Encryption on Law Enforcement and Public Safety

Thank you Mr. Chairman and members of the Committee for providing me with this opportunity to discuss with you an issue of extreme importance and of great concern to all of law enforcement, both domestically and abroad -- the serious threat to public safety posed by the proliferation and use of robust encryption products that do not allow for timely law enforcement access and decryption.

First and foremost, the law enforcement community fully supports a balanced encryption policy that satisfies both the commercial needs of industry and law abiding individuals for robust encryption products while at the same time satisfying law enforcement's public safety needs. On the one hand, encryption is extremely beneficial when used legitimately to protect commercially sensitive information and communications. On the other, the potential use of such robust encryption products by a vast array of criminals and terrorists to conceal their criminal communications and information poses an extremely serious and, in my view, unacceptable threat to public safety. Recently, the President of the International Association of Chiefs of Police sent a letter to President Clinton expressing support for a balanced encryption policy that addresses the public safety concerns of law enforcement. Additionally, the

National Sheriff's Association enacted a resolution last month also expressing their support for a balanced encryption policy and opposing any legislative efforts that would undercut the adoption of such a balanced policy.

Since 1992, when AT&T announced its plan to sell a small, portable telephone device that would provide users with low-cost but robust voice encryption, public policy issues concerning encryption have increasingly has been debated in the United States. Since then, people concerned about privacy, commerce, computer security, law enforcement, national security, and public safety have participated in the dialogue regarding cryptography. On the international front, this past December, the multi-national Organization for Economic Cooperation and Development (OECD) meeting in Paris, France, convened an Experts Group to draft global cryptography principles, thus reflecting an increased global interest in and concern about the use and availability of encryption that can be used to endanger a nation's public safety and national security.

In addition, several Members of Congress have also joined this public discussion by introducing legislation which essentially would remove existing export controls on encryption and which would promote the widespread availability and use of any type of encryption product regardless of the impact on public safety and national security. However, the impact of these bills, should they be enacted, has not been lost on other Members of Congress as reflected in the letters to the sponsors of both Senate encryption bills by the Chairman and Vice-Chairman of the Senate Select Committee on Intelligence. Senators Specter and Kerrey indicated in their letters that they had concerns regarding these bills and expressed the opinion, which I fully endorse, that there is a "... need to balance U.S. economic competitiveness with the need to safeguard national security interests." To that balance, I would also add public safety and effective law enforcement.

Without question, the use of strong cryptography is important if the Global Information Infrastructure (GII) is to fulfill its promise. Data must be protected -- both in transit and in storage -- if the GII is to be used for personal communications, financial transactions, medical care, the development of new intellectual property, and a virtually limitless number of other applications. Our support for robust encryption stems from a commitment to protecting privacy and commerce.

But we are also mindful of our principal mission responsibilities: protecting America's public safety and national security in the myriad of criminal, terrorist, and espionage cases that confront us every day. Notwithstanding the accepted benefits of encryption, we have long argued that the proliferation of unbreakable

encryption -- because of its ability to completely prevent our Nation's law enforcement agencies from understanding seized computer files and intercepted criminal communications which have been encrypted and then being able to promptly act to combat dangerous criminal, terrorist, and espionage activities as well as successfully prosecute them -- would seriously and fundamentally threaten these critical and central public safety interests. The only acceptable answer that serves all of our societal interests is to foster the use of "socially-responsible" encryption products, products that provide robust encryption, but which also permit timely law enforcement and national security access and decryption pursuant to court order or as otherwise authorized by law.

Law enforcement is already beginning to encounter the harmful effects of conventional encryption in some of our most important investigations:

- **In the Aldrich Ames spy case, where Ames was told by his Soviet handlers to encrypt computer file information to be passed to them.**
- **In a child pornography case, where one of the subjects used encryption in transmitting obscene and pornographic images of children over the Internet.**
- **In a major drug-trafficking case, where one of the subjects of one of the court-ordered wiretaps used a telephone encryption device which frustrated the surveillance.**
- **Some of the anti-Government Militia groups are now advocating the use of encryption as a means of preventing law enforcement from properly investigating them.**

It is important to understand, as one can see from the cases I have cited, that conventional encryption not only can prevent electronic surveillance efforts, which in terms of numbers are conducted sparingly, but it also can prevent police officers on a daily basis from conducting basic searches and seizures of computers and files. Without an ability to promptly decrypt encrypted criminal or terrorist communications and computer files, we in the law enforcement community will not be able to effectively investigate or prosecute society's most dangerous felons or, importantly, save lives in kidnappings and in numerous other life and death cases. We simply will not be able to effectively fulfill our mission of protecting the American public.

In a very fundamental way, conventional encryption has the effect of upsetting the delicate legal balance of the Fourth Amendment, since when a judge issues a search warrant it will be of no practical value when this type of encryption is encountered. Constitutionally-effective search and seizure law assumes, and the American public fully expects, that with warrant in hand law enforcement

officers will be able to quickly act upon seized materials to solve and prevent crimes, and that prosecutors will be able to put understandable evidence before a jury. Conventional encryption virtually destroys this centuries old legal principle.

There is now an emerging opinion throughout much of the world that there is only one solution to this national and international public safety threat posed by conventional encryption -- that is, key escrow encryption. Key escrow encryption is not just the only solution; it is, in fact, a very good solution because it effectively balances fundamental societal concerns involving privacy, information security, electronic commerce, public safety, and national security. On the one hand, it permits very strong, unbreakable encryption algorithms to be used, which is essential for the growth of commerce over the GII and for privacy and information security domestically and internationally. On the other hand, it permits law enforcement and national security agencies to protect the American public from the tyranny of crime and terrorism. We believe, as do many others throughout the world, that technology should serve society, not rule it; and that technology should be designed to promote public safety, not defeat it. Key escrow encryption is that beneficial and balanced technological solution.

American manufacturers that employ encryption in their hardware and software products are undoubtedly the technology leaders in the world. American industry has the capability of meeting all of society's basic needs, including public safety and national security, and we, as responsible government leaders, should be sending a clear signal to industry encouraging them to do so. Key escrow encryption is "win-win" technology for societies worldwide. I know you agree that it would be irresponsible for the United States, as the world's technology leader, to move towards the adoption of a national policy that would knowingly and consciously unleash on a widespread basis unbreakable, non-key escrow encryption products that put citizens in the U.S. and worldwide at risk.

Unfortunately, in recent months, the nearly exclusive focus of the public discussion concerning the encryption issue has been on its commercial aspects, particularly with regard to removing export controls. This narrow focus ignores the very real threat that conventional, non-key escrow encryption poses both domestically and internationally to public safety. We continue actively to seek industry's cooperation, assistance, and great expertise in producing key escrow encryption products as a critical part of an overall, balanced, and comprehensive encryption policy that would logically include an appropriate relaxation of export controls for key escrow products.

As for export controls, we have had ongoing discussions with industry, and industry has articulated the view that export controls needlessly hurt U.S. competitiveness overseas. But once again we need to carefully consider the facts and balance a number of competing interests. Although some strong encryption products can be found overseas, they are simply not ubiquitous, and, as of yet, they have not become embedded in the basic operating systems and applications found overseas.

Importantly, when the U.S. recently let it be known that it was considering allowing the export of encryption stronger than that now permitted, several of our close allies expressed strong concerns that we would be flooding the global market with unbreakable cryptography, increasing the likelihood of its use by criminal organizations and terrorists throughout Europe and the world, and thereby imperiling the public safety in their countries. Ironically, the relaxation of export controls in the U.S. may well lead to the imposition of import controls overseas. The international implications and likely reactions of foreign governments to the U.S. unilaterally lifting such export controls must be fully considered.

Given the fact that the use and availability of robust encryption is an issue of concern internationally, it is important to understand what steps other countries are taking to address these concerns. Recently, France, Russia and Israel have established domestic restrictions on the import, manufacturer, sale and use of encryption products, as not to endanger their public safety and national security. The European Union is moving towards the adoption of a key recovery-based key management infrastructure similar to that proposed for use within the United States. This plan, based upon the concept of using a "Trusted Third Party," allows for encryption keys to be escrowed with an independent but non-governmental party, thus allowing for lawful government access to such escrowed key pursuant to proper legal authority.

Lastly, we have heard the oft-repeated argument that the &#65533;genie is out of the bottle,&#65533; and that attempts to influence the future use of cryptography are futile. This is simply not true; and we strongly disagree. If strong, key escrow encryption products proliferates both overseas and domestically which will not interoperate (at least in the long-term) with non-key escrow products, then escrowed encryption products will become the worldwide standard and will be used by almost everyone, including the criminal elements, in countries participating in the GII. It is worth noting that we have never contended that a key escrow regime, whether voluntarily or mandatorily implemented, would prevent all criminals from obtaining non-key escrowed encryption products. But

even criminals need to communicate with others nationally and internationally, including not just their criminal confederates but also legitimate organizations such as banks. Accessible, key escrow encryption products clearly will be used by most if widely available, inexpensive, easy to use, and interoperable worldwide.

In closing, if one considers the broad range of public safety responsibilities that fall upon the law enforcement community, there is only one responsible course of action that we as government leaders must embark upon -- to promote socially-responsible encryption products, products that contain robust cryptography but which also provide for timely law enforcement access and decryption -- that is, key escrow encryption. The entire law enforcement community believes not only that the removal of export controls for encryption products that are non- law enforcement accessible is unwise, but that such an action would jeopardize our national security and the interests and safety of law-abiding citizens worldwide.

We look forward to working with you and your staff on this difficult issue and would be pleased to answer any questions you might have.