Summary - Testimony
House Committee on the Judiciary
Hearing on H.R. 3011, 25 September 1996
William P. Crowell, Deputy Director, National Security Agency

Encryption is a significant potential benefit to U.S. - Need to take steps to maximize potential. - Must mutually acknowledge interests, roles and responsibilities of both industry and governments. - Challenges to address collaboratively: establishment of key management infrastructure (KMI); key recovery capability.

Infrastructure needed to support widespread use of encryption. - KMI facilitates widespread use of encryption; allows encryption to be used with confidence. - Administration's KMI-focused approach: helps KMI grow; addresses public safety interests; helps open doors for U.S. encryption overseas.

Global solution depends on industry/government collaboration. - Administration policy enables industry and government to work together to develop and build infrastructure for managing encryption keys. - Industry: contributes market knowledge and infrastructure technology Government: contributes KMI expertise; in-place working relationships with foreign governments.

Myths and distractions in encryption debate delay resolution of hard problems. - Product "availability": encryption widely available but not widely used; bad metric for basing policy decisions. - Short-sighted to base long-term encryption policy on bit lengths and brute force attacks. Encryption technology can be made intractable against sheer compute power. - The Administration's proposal is not "Clipper III". Much progress has been made towards eliminating contentious issues.

U.S. encryption policies are addressing concerns that the rest of the world is facing. - All countries that are major producers of cryptography control its export; some countries control import and domestic use. - Other countries concerned about domestic public safety. - European Union considering Trusted Third Party architecture.

Congressional action at this time would preempt Administration attempts to reach cooperative agreement with industry.

Administration's policies will have significant impact on NSA but represent a reasonable response to complex, interdependent set of issues.

*****

Introduction

I appreciate the opportunity to comment on Congressman Goodlatte's pending legislation and to discuss with you NSA's involvement with the development of the Administration's encryption policy. Since NSA has both an information security and a foreign signals intelligence mission, encryption touches us directly.

NSA's role in support of the Administration's initiative has been that of a technical advisor. I believe it is important for the nation's encryption policy makers to base their decisions on the best possible information, and I would like to help clarify several issues for the record.

Encryption Is a Significant Potential Benefit To America

The use of encryption to protect U.S. information should be promoted, not discouraged. Encryption usage has the potential to enable citizens

to use technology that will make their lives more convenient, enhance the economic competitiveness of U.S. industry, combat frivolous and criminal access to private and valuable information, and deny spies from gaining access to U.S. information wherever it may be in the world. That's the good news. The bad news is that the encryption in most commercial products today has very little chance of being used to its full potential until a support infrastructure is established that enables the encryption to be used widely and with integrity. Furthermore, if encryption is used by criminals and other adversaries (e.g., terrorism) to help hide their activities, the public safety of U.S. citizens, and citizens of other countries, may be placed in jeopardy. This is a problem regardless of whether a support infrastructure exists or not.

The U.S. must address these challenges. Instead, we seemed mired in an unfocused debate aboutbit lengths, brute force attacks, and product "availability" that often takes place in press releases, newspaper editorials, and Internet Newsgroups. We all need to focus-in on what will enable encryption to be used to its potential. The way to do this is to mutually acknowledge the interests, roles, and responsibilities that industry and governments have in this issue. Specifically, the two challenges that we must address collaboratively are:

- The establishment of a trustworthy key management infrastructure (KMI) that facilitates encryption that is interoperable, scatable, and enables the encryption to be used to its full potential.

- The ability to recover an encryption key when that key is needed by the user or others who are authorized to have it.

An Infrastructure Is Needed To Support The Widespread Use Of Encryption

The KMI is the keystone of the Administration encryption policy reform proposal since encryption has little chance of becoming widely used, here or overseas, until there is such an international framework in place. When I use the term "key management infrastructure" I am referring to the policies, products, and services that, in total, provide a support infrastructure for end-user products that contain encryption. A KMI includes functions such as distributing encryption certificates that can help vouch for your identity, storing information that allows others to know how to communicate with you, assisting you when you have reasons to believe that your encryption certificate has been cornpromised, and other objectives. The goal of such a support infrastructure or "KMI" is to facilitate widespread use of encryption and allow the encryption to be used with confidence. The system integrityfostered by such an infrastructure will allow us to have the same confidence in electronic commerce that we now have in signatures on paper contracts or in handshakes with business partners, and is needed to achieve our vision of global commerce with secure interoperability.

A national framework does not exist today, other than in the KMI used by the Defense Department and other specialized areas. The Administration's recommended KMI-focused approach intends to help fill that void by helping the U.S. KMI grow, addressing the nation's public safety interests, and helping open doors for U.S. encryption overseas.

-- Helping the KMI Grow - First, the Administration wants to help ensure that the U.S. KM/ allows encryption to be used securely, widely, and with confidence. We recognize that the emergence of a commercial KMI is inevitable but are concerned that infrastructure users and public safety will be placed at risk if it grows in the wrong direction, thereby harming the public's interests.

-- Information protection - To ensure adequate protection of sensitive information, the KMI needs to be built and operated securely. Furthermore, a sealable infrastructure is needed to support large numbers of encryption users, and it must facilitate interoperability.

-- Data recovery - Users will need the capability to regain access to their encrypted data when encryption keys are lost, corrupted, or destroyed. The KMI must therefore support key recovery. While key recovery may not yet be widely recognized as a user requirement, analogies to key recovery are common in the workplace. Today, computer system administrators help users recover their forgotten passwords. Similarly, most offices securely maintain spare door and desk keys for emergency use.

-- Privacy - Regulations must be established to ensure that access to keys is not misused to violate individual privacy.

- Addressing the Nation's Public Safety Interests and Helping to Open Doors for U.S. Encryption Products Overseas - Second, the Administration wants to ensure that the KMI supports our government's responsibility to protect the nation's public safety, and provide a level playing field on which U.S. products can compete overseas.

-- Public Safety Protection - While users should have the ability to choose responsible agents to generate and store their keys, government's public safety responsibilities will require law enforcement, with proper authorization, to be able to gain access to keys. Without key recovery, law enforcement agencies will be unable to decrypt encrypted criminal files and communications. The Administration proposes to use the KMI's data recovery feature to support authorized law enforcement investigations, rather than creating a separate infrastructure that solely supports those investigations.

-- Export Control Reform - If the KMI supports key recovery, then bit limit restrictions can be lifted on encryption exports, and other countries will be less likely to institute import restrictions on U.S. encryption since foreign government interests can also be met by key recovery in the KMI.

-- Foreign Sales - The U.S. government intends to promote the advantage of key recovery solutions to foreign governments.

A Global Solution Depends On Industry/Government Collaboration

The Administration's encryption policy would, I believe, satisfy a balanced cross-section of society's needs. In broad strokes, this policy enables industry and government to work together to develop and build the infrastructure for managing encryption keys. Industry can bring their market knowledge and infrastructure technology and services to the collaborative effort, while the U.S. government can contribute decades of KMI expertise, and extensive in-place working relationships with foreign governments.

The Administration has engaged various industry and international groups to further define the infrastructure concept. All agree that the emergence of a KMI is necessary. Some in industry, however, continue to seek immediate relaxation of existing export controls on encryption. The Administration is now discussing with industry a variety of proposals for export control relaxation. The Administration is mindful that such relaxation should be consistent with the objective of encouraging the development of a robust, full-featured, key management infrastructure that supports key recovery. It would be a terrible irony if this government -- which prides itself on its leadership in

fighting international crime -- were to enact a policy that would jeopardize public safety and national security, as well as weaken law enforcement agencies worldwide.

Myths And Distractions In The Encryption Debate

The encryption debate has often been mischaracterized as a struggle between high-tech industry which wants to sell encryption products worldwide, and the government which is perceived as wanting to prevent the spread of encryption. Such myths, and other threads of the encryption debate, are unsound. They do not address the issues at hand, they can cause unnecessary conflicts among thosethat are pursuing them, and they ultimately delay the resolution of the hard problems. These myths and distractions include product availability, brute force attacks, and comparisons to the Clipper initiative.

- Product "Availability" Is A Bad Metric For Basing Policy Decisions

Most measurements of product availability are inadequate (incomplete or inconclusive) since they do not show how many people are using encryption. Product availability can be measured in a number of ways. Depending on how it is measured, one could misconstrue the data to

conclude that "the encryption genie is out of the bottle" or that the bottle is tightly plugged. The fact of the matter is that encryption is widely available (e.g., embedded in tens of millions of commercial software products) but is not widely used.

Those who argue that government encryption policies are outdated because "the encryption genie is out of the bottle" (i.e., there are many products advertised to contain encryption and some of them are available from the Internet) must consider three important perspectives.

First, encryption is not, and will not be used widely and to its potential (with confidence by 100s of millions of people) until there is an infrastructure in place to support it. Encryption is usually not used because there is not an infrastructure in place to support the distribution of keys among the users of the products, its key/certificate management often lacks robust integrity, and it cannot be scaled to support large communities of interoperable communicators. Furthermore, the products are usually not interoperable. Today, if the encryption is used at all, it is used very narrowly.Encryption is not a genie that will magically solve the security problem and the Administration is not trying to 'keep the plug in the bottle'. The Administration wants to help promote a full range of trusted security services providing privacy, authentication, and data integrity while simultaneously helping our government, and

governments worldwide, uphold their public safety and national security responsibilities.

Second, serious users of security products don't obtain them from the Internet. The president of a prominent Internet security corporation was recently asked in a magazine article on this issue: "Since encryption technology is available as freeware off the Internet, why would anyone pay a company for it?" He responded by saying: "Freeware is worth exactly what you pay for it. I'd rather not implement security systems using software for which the source code is available to any 12-year-old who thinks being a hacker is fun."

Third, the Internet does not make the distribution of software-based products, including encryption, uncontrollable. Most people elect to obtain their software from legal sources to ensure they do not violate the law, and so that they can obtain essential product support from software developers. Yes, some people illegally violate copyright laws when they place commercial software on the Internet, and some people violate export laws when they place encryption software on the Internet. However, these illegal actions on the Internet constitute a very small percentage of the market.

- It Is Short-Sighted To Base Long-Term Encryption Policy On Bit Lengths And Brute Force Attacks

some have argued that law enforcement and intelligence agencies can build special-purpose,high-performance computers to enable them to read encrypted communications. These computers would "break" encryption systems via "brute force" attacks. This line of argument is

a distraction from the real issues at hand, and I encourage you to consider the following information and put this debate behind us.

NSA has decades of experience in designing such high performance machines. Though it would be intellectually stimulating to discuss assumptions on the design of such theoretical machines, I think a compelling argument against relying on brute force attacks is made by accepting the estimates for the performance theoretical machines.

Suppose that the theoretical machine were asked to assist law enforcement to decrypt a message encrypted by a terrorist organization and that organization used the algorithm in PGP (Pretty Good Privacy), an encryption package available on the Internet. That law enforcement investigation would be delayed for quite a long time, since the theoretical machine would take longer than the estimated age of the universe (15 billion years) to recover a single message via brute force. In fact, it would take an

estimated 100,000,000,000,000,000 (100 quadrillion) years to recover that message, over six million times the estimated age of the universe. Moreover, it is important to note that modern cryptographic systems generate a unique key for each new message; therefore, each subsequent message would require the same amount of effort.

Clearly, encryption technology can be made intractable against sheer compute power, and longterm policies cannot be based on bit lengths. Brute force attacks cannot be the primary solution for law enforcement decryption needs.

- The Administration's Approach To Encryption Policy Reform Is Very Different From Earlier Key Escrow Initiatives (E.g., Clipper)

Some have incorrectly labeled the Administration's proposal 'Clipper III'. Their argument is disingenuous. The Administration's proposal differs significantly from previous key escrow initiatives since it eliminates the focus on bit lengths and promotes the development of a KM1 that can help spread commercial encryption. The following chart identifies six major criticisms with the Clipper initiative and the 64 Bit Software Key Escrow initiative, and compares them to the policies defined by the Administration in its KM/proposal.

**Table not transmittable

With these impediments addressed, industry and government can work to establish encryption products that will win acceptance in foreign markets and establish infrastructure services to support those products.

The U.S. government and U.S. industry share a common goal regarding foreign markets: eachseeks a level playing field upon which U.S.

products can fairly compete. This Administration believes that that goal can, and must be reached while also addressing law enforcement and foreign government interests via key recovery.

U.S. Encryption Policies Are Addressing Concerns That The Rest Of The World Is Also Facing

All countries that are major producers of cryptography control its export. Though the U.S. does not have domestic restrictions, some countries control the import of encryption and its domestic use. Recently, France, Israel, and Russia imposed import and domestic use restrictions, and several Asian, South American, and African countries have done so for many years.

Some countries have already expressed concern and may resort to raising import barriers to U.S. products if U.S. export policies change radically. They are concerned about the public safety impact to their countries if criminal elements use encryption to thwart public safety efforts.

The European Union (EU) is considering a key recovery-based key management infrastructure to address the expected growth in the demand for commercial encryption. The EU plan, known as the Trusted Third Party or TTP architecture, protects EU governments' public safety interests by ensuring that keys are stored with a party other than the originator of the encrypted information. Other confederations and organizations are also approaching the encryption issue by including a key recovery feature. For example, the major standards bodies of the world are designing future standards so that key recovery can be accommodated. The U.S. is not the only place that recognizes the dual- edges of the encryption tool.

Wrap Up

The Administration is basing its policies on the foundation that the need for robust commercial encryption will grow and has proposed policy reforms to ensure that American companies, and the public, can flourish in the future encryption market. The Administration 's approach is not past its time, it is just in time. The fundamental issue in play is how industry will build a key management infrastructure to support mass market products with encryption. If an infrastructure is built that supports key recovery, then the export control debate can be concluded. Otherwise, governments worldwide are likely to resist the use of those products because of public safety concerns.

This is where the Administration needs your help. Congressional action at this time would preempt Administration attempts to reach a cooperative agreement with industry that satisfies all interested parties. It would also result in the world-wide proliferation of secure encryption that is contrary to the public safety interests of the U.S. and other nations.

Though the Administration's proposed policies will have a significant impact on NSA, I believe they are a reasonable response to a complex, interdependent set of issues. I hope that the Administration can continue to work with Congress and industry to reach a resolution of these issues. Thank you for the opportunity to address this important matter.