PREPARED STATEMENT OF WILLIAM P. CROWELL, DEPUTY DIRECTOR, NATIONAL SECURITY AGENCY

Security and Freedom Through Encryption (SAFE) Act
March 20, 1997 - House Judiciary Subcommittee on Courts and Intellectual Property

PREPARED STATEMENT OF WILLIAM P. CROWELL, DEPUTY DIRECTOR, NATIONAL SECURITY AGENCY

INTRODUCTION

I appreciate the opportunity to comment on the pending Pro-CODE 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. For decades, NSA has been the nation's center of cryptographic expertise. We have played an important role in using cryptography to produce the safeguards that control our nuclear arsenal, enable our military commanders and policy makers to communicate securely anywhere in the world, provide our intelligence customers with vital information to support U.S. interests, and protect classified and sensitive-but-unclassified information. 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.

THE USE OF ENCRYPTION CAN BE A SIGNIFICANT BENEFIT TO AMERICA

The country is now engaged in a national discussion on encryption centered on how to accommodate the private interests of individuals and businesses with the public interests of law enforcement and national security. How we resolve this will affect how well the nation succeeds in the information age.

Some would argue that if we overemphasize the public interests, we risk a world with too much government access and too few secrets. Others argue that if we overemphasize the interests of the private sector, we risk a world with perhaps too many secrets—for example, a world in which terrorists, organized crime, and hackers acquire the capability to operate with impunity. Both of these extremes are unpalatable and are therefore not part of the Administration's policy. We need to strike a balance that provides adequate protection for both individuals and businesses, and for society as a whole.

The White House recently defined a policy initiative that is designed to accelerate growth in the use of encryption. Some believe the administration's initiative is about key recovery and export controls, but in the broadest sense the initiative deals with the preparations we must make as a nation to use information technology to its full potential. It transcends the key recovery issue. It focuses on the more fundamental question of key management infrastructure (KMI). In other words, it is an attempt to create an international framework in which the use of strong encryption will grow. I cannot overemphasize either the importance or the difficulty of moving this initiative from concept to reality.

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 adversaries 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., terrorists) 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 whether a support infrastructure exists, or not.

The U.S. must address these challenges. Instead, we seem mired in an unfocused debate about bit 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.

OVERVIEW OF KEY MANAGEMENT INFRASTRUCTURE AND PUBLIC KEY ENCRYPTION

Crypto products use algorithms and keys to encrypt and decrypt information. The algorithm combines the key with the information that a person wants protected or authenticated. The keys must be unique, random number streams generated by a trusted authority and delivered by a trusted means to the users. The system of people and processes that provide these services is called a *key management infrastructure (KMI),* and it enables keys to be generated properly, securely transported, authenticated, and stored.

For years, secure KMIs consisted of people hand-delivering keys to each pair of potential communicators. Such a secure KMI became impractical when a large number of people needed to potentially communicate. Furthermore, security was often degraded when keys were compromised during the delivery stage. Even computer delivery of keys did not solve these problems. In general, the use of encryption was not widespread because of these KMI complexities and limitations.

A type of encryption technology called *public key technology* was invented to address the KMI scalability problem and reduce the possibility of key compromise during delivery. Public key encryption does not eliminate the need for a KMI, it only changes what products and services we expect from the infrastructure.

A *public key infrastructure (PKI),* a type of KMI, does not require shared, confidential keys to be pre-placed in order for people to communicate. Instead, it uses two related keys—a public key and a private key—and allows the public encryption key to be made known and stored in publicly-accessible places. There is no magic involved, only the use of complex mathematics and other techniques to effectively hide the part of the key that must be kept secret.

A PKI's services are for: 1. Verifying user identities; 2. generating user public and private key pairs; 3. linking user identities with their keys; 4. accessing the database of user identities & keys; 5. verifying the integrity of user identities & keys; 6. deleting invalid user identities & keys; and 7. dealing with compromised or lost keys.

All of the above services are necessary to enable public key-based encryption products to be used widely, securely, and with integrity. The certification of the public key value for each individual using public key encryption is the absolute foundation of trustworthy public key encryption. Without this certification service, users of computer networks have no way of verifying who they are talking to or who has signed documents or commercial transactions in digital transactions.

AN INFRASTRUCTURE IS NEEDED TO SUPPORT THE WIDESPREAD USE OF ENCRYPTION

Today, businesses hope to use encryption to expand into the ''new world'' of electronic commerce (EC), but the lack of a robust KMI leaves EC pioneers shortchanged. For this reason, the KMI is the keystone of the Administration encryption policy reform proposal. Encryption has little chance of being used to its fullest potential, here or overseas, until there is an international key management framework in place. Unfortunately, there has been too much emphasis on algorithms and key lengths in the encryption debate. There is much more to the issue of trust than a good encryption algorithm. The algorithm gets you perhaps 5% of the way there. Without a trustworthy infrastructure to support it, an encryption algorithm's value is comparable to that of a bank vault door on a cardboard box. Many commercial information products and services are facing a tide of resistance because of their lack of security or trust.

When I say trust, I mean that you must be willing to bet your company's future not only on the strength of your algorithm, but on the integrity of those who:

Issue the encryption certificates that vouch for your identity and the identity of those you deal with;

Build the directories that allow others to know how to communicate securely with you; and,

Assist you if you believe your encryption key or certificate has been compromised or lost.

Rhetoric aside, there is very little disagreement in the software or hardware industry that KMIs are needed to increase the use of encryption. The system integrity fostered 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 electronic commerce with secure interoperability.

An encryption support infrastructure does not exist today, other than in the KMI used by the Defense Department and other specialized areas where it is essential to the viability of systems. The Administration's recommended KMI-focused approach intends to help fill that void by helping U.S. KMIs to grow, addressing the nation's public safety interests, and helping to open doors for U.S. encryption overseas.

THE KMI'S WILL NEED TO SUPPORT KEY RECOVERY

As the EC pioneers build KMIs to support large numbers of encryption users, they will need to provide the capability to regain access to their encrypted data when encryption keys are lost, corrupted, destroyed, or otherwise unavailable. This feature, commonly referred to as ''key recovery,'' is a means to ensure greater safety and trust, and there are compelling business reasons for it. Key recovery ensures, for example, that:

Employees can recover encrypted E-mail or files in the event that the disk that holds their encryption key crashes;

Corporations are not held hostage to a disgruntled employee who sabotages company files by encrypting valuable company intellectual property; and,

Companies can pass accounting audits, even if archived data had been encrypted with an expired encryption key.

The KMI is a logical place to 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 of flees securely maintain spare door and desk keys for emergency use.

Certainly users should have the ability to choose their own responsible agents to generate and store their keys, but the government's public safety responsibilities will require that law enforcement, with proper authorization, to be able to gain access to such keys. Without key recovery, law enforcement agencies will be unable to decrypt encrypted criminal files and communications since modern commercial encryption can prevent computerized ''brute force attacks'' against the criminal communications. The Administration proposes to use privately operated KMI data recovery features to support authorized law enforcement investigations, rather than creating a separate infrastructure that solely supports those investigations.

A GLOBAL SOLUTION DEPENDS ON INDUSTRY/GOVERNMENT COLLABORATION

The Administration's encryption policy satisfies a cross-section of society's needs. The policy enables industry and government to work together to develop and build the infrastructures 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 mindful that any such relaxation must be consistent with the objective of encouraging the development of a robust, full-featured, key management infrastructure that supports key recovery.

MYTHS AND DISTRACTIONS IN THE ENCRYPTION DEBATE

I would like to help clarify some of the frequently-repeated factual errors regarding encryption so we all can stand on firm ground during the formation of the nation's encryption policies.

The encryption debate has often been mischaracterized as a struggle between the high-tech industry, which wants unlimited freedom 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 the parties to the debate, and they ultimately delay the resolution of the hard problems. These myths and distractions include brute force attacks, comparisons to earlier key escrow initiatives, and encryption availability and use.

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

You may have heard news accounts of a University of California Berkeley student who recently decrypted a message that was encrypted with a 40-bit key using 250 workstations as part of a contest from RSA Inc. This so-called ''challenge'' is often cited as evidence that the government needs only to conduct ''brute force'' attacks on messages when they are doing a criminal investigation. In reality, law enforcement does not have the luxury to rely on headline-making brute force attacks on encrypted criminal communications. I think you will find it useful to see for yourselves how increased key sizes can make encryption virtually unbreakable. Ironically, the RSA challenge proves this point.

If that Berkeley student was faced with an RSA-supplied task of brute forcing a single PGP based (128-bit key) encrypted message with 250 workstations, it would take him an estimated 9 trillion times the age of the universe to decrypt *a single message.* Of course, if the Berkeley student didn't already know the contents of part of the message—RSA provided some of the unencrypted message content to assist those who accepted the challenge—it would take even longer.

For that matter, even if every one of the 29,634 students enrolled at UC Berkeley in 1997 each had 250 workstations at their disposal—7,408,500 computers (cost: $15B)—it would still take an estimated 100 billion times the age of the universe, that is over 1 sextillion years (1 followed by 21 zeros), to break a single message.

If all the personal computers in the world—260 million computers—were put to work on a single PGP-encrypted message, it would still take an estimated 12 million times the age of the universe, on average, to break a single message (assuming that each of those workstations had processing power similar to each of the Berkeley student's workstations).

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. This line of argument is a distraction from the real issues at hand, and I encourage you to help put this debate behind us.

Table 1

TABLE 1

ESTIMATED TIME NEEDED TO RECOVER A SINGLE KEY USING THE 250 WORKSTATIONS USED BY THE BERKELEY STUDENT WHO SOLVED RSA'S 40-BIT CHALLENGE*

Number of Bits	Average Time	Time If Key Is Found 1/3 of the Way Through the Full Exhaust**
40	5.5 hours	3.6. hours.
56	41 years	27 years.
64	11 thousand years	7 thousand years.
80	690 million years	455 million years.
128	13 trillion times the age of universe	9 trillion times the age of the universe.

*RSA gave away part of the decrypted text to those trying to solve the challenge.
**Berkeley student recovered RSA Challenge 40-bit key 33% into exhaust attack.
Average point at which a key is recovered during an exhaust attack = 50%.
Berkeley student performed 100 billion operations per hour using 250 workstations.
Age of the universe = 15 billion years.

The Administration's Approach To Encryption Policy Reform Is Very Different From Earlier Key Escrow Initiatives

Some have argued that the Administration's recent policy initiative is the same as previous key escrow initiatives. Their argument is disingenuous and incorrect. The KMI initiative is about creating an environment in which commercial encryption can flourish. Just as significant, the Administration's proposal differs significantly from previous key escrow initiatives because: It eliminates the focus on bit lengths; the government doesn't hold the keys; a separate key escrow infrastructure is not required; keys can be held overseas; it doesn't prescribe algorithms or limit them to hardware; and users' data recovery needs can be met.

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

Several major companies recognize these profound changes and have formed business ventures to thrive within the new climate. In October 1996 IBM formed the *Key Recovery Alliance* and that alliance has already grown to over 50 domestic and international companies. Alliance members include America Online, Apple, Mitsubishi, Boeing, DEC, Hewlett Packard, Motorola, Novell, SUN, Unisys, and RSA.

Despite Being Available, Encryption Is Not Being Widely Used

Most measurements of encryption are inadequate (incomplete or inconclusive) since they do not show how many people arc using encryption. Encryption 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, based on our impressions from market surveys, etc., *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 two important perspectives.

First, *encryption is not now being, and will not be used to its fullest potential (with confidence by 100s of millions of people) until there is an infrastructure in place to support it.*

Encryption is not a genie that will magically solve the security problem. Nor is the

Administration 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 fulfilling public safety and national security responsibilities for our government, and governments worldwide.

Second, *serious users of security products don't use free security products 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.'' In other words, when determining what encryption you use to protect valuable business secrets, you should consider who you're getting it from, how it got to you, and whether you'll receive support when you need it.

U.S. ENCRYPTION POLICIES ARE ADDRESSING CONCERNS THAT THE REST OF THE WORLD IS ALSO FACING

The U.S. is not the only nation which has concerns that encryption use by criminals can threaten public safety. All countries that are major producers of cryptography control its export. Some of those countries have voiced their displeasure with the U.S. decision to export 56-bit encryption. Though the U.S. does not have domestic restrictions, some countries do through import controls 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 informally done so for many years.

At this point, it would be overgeneralizing to say that the world has agreed to an approach on key recovery, but it is accurate to say that all governments want authorized access to encrypted information. The U.S. is not the only nation that recognizes the dual-edged nature 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 it 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.

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.