

The Third CPSR Cryptography and Privacy Conference

Source Book

**June 7, 1993
Washington, DC**

Computer Professionals for Social Responsibility

**The Third
CPSR
Cryptography
and Privacy
Conference**

Source Book

David Banisar and Marc Rotenberg, editors

**CPSR Washington Office
666 Pennsylvania Ave, SE
Suite 303
Washington, DC 20003
@washofc.cpsr.org**

June 1993

This year marks the third CPSR Cryptography and Privacy conference. This conference begins just as a series of public meetings at the Department of Commerce on cryptography policy have concluded. We hope to continue the discussion and to provide an opportunity for interested parties to exchange views directly with one another and to answer questions.

It should be clear at this point that the policies developed in our country on the use of cryptography will have far-reaching implications. Who builds the locks and who has access to the keys are now central questions. But even as the current debate explores the rights of privacy, the development of commercial products, and the needs of law enforcement, we should anticipate that new issues will soon follow. How will public key directories be managed? What conventions will be developed for authentication? How will the general public respond to the use of cryptography for routine communications?

We hope that these discussions will help promote more informed policies. We are very pleased that a distinguished group of technical experts and representatives of public interest and private organizations are taking part. We especially appreciate the participation of staff members from the federal agencies, Congressional committees and the White House directly involved in the development of current policy. It is critical to the integrity of the policy process that public concerns be heard in an open forum and not behind closed doors.

As in the past, CPSR policy analyst Dave Banisar should get full credit for developing the program, bringing together an outstanding group of participants, and compiling the materials for the source book. The significance of this conference has grown in large measure due to Dave's efforts.

CPSR's work on cryptography policy has also benefited from the efforts of Legal Counsel David Sobel who has litigated Freedom of Information Act cases against the National Institute of Standards and Technology, the National Security Agency, and the National Security Council. While we recognize that these cases have sometimes caused heartache for agency officials, we believe that the disclosure of important government documents is necessary for a fully informed public debate. In just the past year, CPSR has obtained the previously classified directive on computer security policy, the General Services Administration's assessment of the FBI's digital telephony proposal, and the minutes of the NIST/NSA Technical Working Group meetings. Many of these documents are contained in this source book.

CPSR Washington Office
666 Pennsylvania Ave. S.E.
Suite 303
Washington, DC 20003
202 544-9240
Fax 202 547-5481/2
rotenberg@washofc.cpsr.org

Marc Rotenberg, Director
Richard Cville, Program Director
David Sobel, Staff Counsel

CPSR National Office
P.O. Box 717
Palo Alto, CA 94302
415 322-3778
Fax 415 322-3798
Nikki Draper, Office Manager
cpsr@csli.stanford.edu

CPSR Cambridge Office
P.O. Box 962
Cambridge, MA 02142
617 864-7329
Gary Chapman, Director
chapman@saffron.lcs.mit.edu

Advisory Board
Herbert L. Abrams
John Backus
Paul Brest
David Burnham
Dorothy Denning
Carol Edwards
Douglas Engelbart
Admiral Noel Gayler
Adele Goldberg
Richard Karp
Barbara Liskov
Elliot Maxwell
James Martin
Eli Noam
Karen Nussbaum
Severo M. Ornstein
Anthony Ralston
John Shattuck
Herbert Simon
Robert E. Tarjan
Robert W. Taylor
Lawrence Tesler
Sherry Turkle

Board of Directors

President
Eric Roberts

Chairperson
Jeff Johnson

Secretary
Todd Newman

Treasurer
Rodney Hoffman

Directors
Cathy Cook
Paul Hyland
Lesley Kalmin
Patti Lowe
Ivan Milman
Ronni Rosenberg
Douglas Schuler
Dan Williams
Terry Winograd
Coralee Whitcomb

We wish to thank those organizations and individual who support the CPSR Civil Liberties program, including the J. Roderick MacArthur Foundation, the Deer Creek Foundation, the HKH Foundation, and the Mill Stream Fund. Specific support for this conference was provided by W.H. and Carol Ferry, the Fund for Constitutional Government, the Information Technology Association of America and the National Science Foundation (anticipated). The United States Privacy Council and Privacy International expressed their support for this event. We also acknowledge the assistance of Larry Hunter and Paul Hyland of the CPSR/DC chapter as well as Eric Roberts and the CPSR Board of Directors for their continuing support,

We also wish to remember Phil Stern who helped establish the CPSR Washington office and whose generous spirit and dedication to the public interest has remained an inspiration for many of us.

CPSR is a national membership organization with offices in Palo Alto, California, Cambridge, Massachusetts, and Washington, DC. For membership information, please contact the CPSR National office, P.O. Box 717, Palo Alto, CA 94302. The electronic mail address is cpsr@cpsr.org.

Marc Rotenberg, director
CPSR Washington office

OVERVIEW OF CRYPTOGRAPHY POLICY ISSUES

Cryptography

Cryptography is the art of writing messages in code. A simple substitution scheme, such as D for A and P for M, will generate a code. "WHITE HOUSE" becomes "ZKLWH KRXVH." In this example, known as the Caesar code, the code is not very difficult to solve given enough text. But more complex codes are easy to create and computers lend themselves particularly well to encoding and decoding information.

For most of the history of cryptography, the key, or method, that was used to encode a message remained secret. One copy of the key was needed by the sender to encode the message, a second copy of the same key was necessary to decode or unlock the message. However, distributing these secret keys was a problem. Secure channels had to be established before keys could be sent out and encoded messages exchanged. For this reason applications remained primarily limited to military maneuvers and intelligence communications.

The development of public key cryptography in the 1970s made it possible to design cryptographic systems for widespread use. The need for cryptography has also increased as messages have moved from paper to electronic formats and as wireless communications have replaced hard-wired networks.

A number of good texts on cryptography, including D. Denning, *Cryptography and Data Security* and G. Brassard *Modern Cryptography*, are available for those who wish to study the science of computer encoding in more detail. David Kahn's *The Codebreakers* remains the most comprehensive book on the history of cryptography.

Source book

The purpose of this collection of materials is not to offer a technical overview of cryptography. The documents, news items, reports from government agencies, legislative proposals, summary of laws, and public statements are intended to provide an overview of the critical issues in today's policy debate. We have attempted to select materials so that both sides of an issue are fairly presented. We have generally deferred to the proponents and the opponents of a particular proposal and allowed interested parties to speak in their own words. And we have tried to highlight those issues that appear to be of greatest concern to the general public.

Section I begins with several short articles on cryptography and privacy. In the last few years the close link between cryptography technology and privacy protection has become clear. In part this is the result of the growing number of commercial applications for cryptography. But it may also be the anticipation that in the not too distant future cryptography will be the "glue" that seals virtually all electronic mail. For this reason, those who seal letters and those who would open letters are especially interested in the policies governing the development and use of cryptography. For some, as the cypherpunks manifesto suggests, the right to encode may even define a political movement.

Section II looks at the history of the Computer Security Act, a law passed in 1987 that addresses the roles of several federal agencies in the development of technical standards. Because much of the recent debate surrounding cryptography policies has focused on the activities of two agencies – the National Institute of Standards and Technology (NIST) and the National Security Agency — this legal framework has taken on new significance. This section explores the development of the Act, the 1989 Memorandum of Understanding between NIST and NSA, and a Presidential directive issued in 1991. Also included in the section are a series of documents obtained by CPSR through the Freedom of Information Act (FOIA) that trace the activities of NIST and NSA in the development of the Digital Signature Standard, a particular technical standard important for the authentication of computer messages. Minutes from the meetings of the NIST/NSA Technical Working Group as well as agency memos raise important questions about the current operation of the Computer Security Act.

Section III turns to the Clipper proposal, the encryption standard announced by the White House in mid-April, based on a key escrow configuration. The section includes the White House announcement about Clipper, a series of slides prepared by NIST, and several public statements about the proposal. The recently adopted resolutions of the Computer System Security and Privacy Advisory Board conclude the section.

Section IV reviews the FBI digital telephony proposal. Some of the materials may be familiar to people who have followed this issues. The FBI's legislative proposal is included. Also included is a report from the General Accounting Office exploring several issues raised by the plan and a memo from the General Services administration obtained by CPSR through the FOIA. Assessing the importance of wiretap is not a simple task. Items provided on this point include a statistical analysis of the use of wiretaps, a brief paper on the economies of wire surveillance, and polling data from the Department of Justice on public attitudes toward electronic surveillance.

In Section V looks at cryptography and export controls. Firms in the United States continue to face restrictions on the sale of computer hardware and software containing cryptography. The reason for this policy is to allow intelligence agencies in the United States to monitor communications overseas. However, U.S. firms have argued that similar products are available from countries outside the United States and that the current policy cannot be enforced. This section includes key documents surrounding an agreement between the Software Publishers Association and the National Security Council.

Finally, Section VI turns to emerging applications of cryptography. David Chaum's article from *Scientific American* explores a model for electronic privacy in commercial transactions based on "blind signatures." Privacy Enhanced Mail and Pretty Good Privacy are two different configurations to protect computer communications.

Third CPSR Cryptography and Privacy Conference

Source Book Contents

I. Cryptography and Privacy

- Battle for Control of Encryption Technology,
David Banisar, CPSR, *IEEE Software* (July 1993)
- The Only Locksmith in Town,
Index on Censorship (January 1990)
- Proposed Privacy Guidelines for the NREN
Presentation at NCLIS Conference (July 21, 1992)
- The Impact of a Secret Cryptographic Standard on Encryption, Privacy, Law
Enforcement and Technology
Whitfield Diffie, Sun Microsystems (May 11, 1993)
- A Cypherpunk's Manifesto
Eric Hughes (March 9, 1993)

II. Computer Security Act

- Computer Security Act of 1987
- Memorandum of Understanding Between NIST and NSA
- Testimony on Military and Civilian Control of Computer Security before the
Legislation and National Security Subcommittee of the Committee on Government
Operations, House of Representatives
CPSR (May 4, 1989)
- National Security Directive 42*
National Security Council (July 5, 1990)
- Communications Security (COMSEC) Monitoring (NTISSD No 600)*
National Telecommunications and Information Systems Security
- Keeping Fewer Secrets
CPSR, *Issues in Science and Technology* (Fall 1992)
- Letter to Congressman Jack Brooks
CPSR (August 11, 1992)
- Government Restrictions on the Development and Dissemination of Cryptographic
Technologies: The Controversy Over the Digital Signature Standard
David Sobel, CPSR, *Computer Law Reporter* (October 1992).
- Documents Show NSA Dominance of Civilian Computer Security
David Sobel, CPSR (May 6, 1993)
- Selected NSA/NIST Documents Concerning the Development of the Digital Signature
Standard Released in CPSR v. NIST includes minutes of NSA/NIST Technical Working
Group meetings*
- Statement before the Subcommittee on Telecommunications and Finance of the
Committee on Energy and Commerce, House of Representatives
Raymond Kammer, NIST (April 29, 1993)

III. Clipper

Statement by the Press Secretary on Clipper Proposal
The White House (April 16, 1993)
Cryptography, Clipper and Capstone
Dorothy Denning (May 11, 1993)
Statement of CPSR Washington Office Before NIST Hearing (June 2, 1993)
Letter to Secretary of Commerce Ron Brown
Congressman. Edward Markey (April 19, 1993)
Statement Before NIST Hearing by Addison Fischer (June 2, 1993)
Statement of the Computer Business Equipment Manufacturers before NIST Hearing
(May 27, 1993)
Statement of the ACLU before NIST Hearing (May 28, 1993)
Resolutions adopted by the Computers System Security and Privacy Advisory Board of
NIST on Key Escrow and Clipper (June 4, 1993)
Panel Sees Flaws in Plan for Encoding
John Markoff, New York Times (June 5, 1993)
S-266

IV. Digital Telephony

Digital Telephony Proposal
Federal Bureau of Investigation (March 1992)
Digital Telephony Proposal
Federal Bureau of Investigation (May 1992)
Advanced Communications Technologies Pose Wiretapping Challenges
General Accounting Office (July 1992)
Analysis of Digital Telephony Proposal*
General Services Administration (1992)
FBI Proposal on Wiretaps Draws Criticism from GSA
Anthony Ramirez, New York Times (January 15, 1993)
Statistical Analysis of Electronic Surveillance
David Banisar, CPSR (June 3, 1993)
Can Wiretaps Remain Cost-Effective?
Robin Hanson (May 21, 1993)
Public Attitudes Towards Wiretapping
US Department of Justice, Source book of Justice Statistics (1990)

V. Export Controls

Encryption Export Controls
David Peyton, ICOT (June 7, 1993)
Testimony on National Cryptography Policies
Ilene Rosenthal, SPA (June 3, 1993)

Letter to Congressman Valentine

Vinton Cerf, INET (April 11, 1993)

SPA Supports Relaxed and Streamlined Export Controls of Encryption Software Issued
by Bush Administration

Software Publishers Association (July 17, 1992)

Letter to Senator Jake Garn

Brent Scowcroft, National Security Council

Letter to Admiral McConnell, NSA

Richard Clarke, State Department (July 5, 1992)

Federal Register Amendment to the International Traffic in Arms Regulations (ITAR),
the US Munitions List (July 20, 1992)

VI. Uses of Cryptography

Achieving Electronic Privacy

David Chaum, Digicash, *Scientific American* (August 1992)

Internet Privacy Enhanced Mail (PEM)

Steven Crocker, TIS (June 1993)

Pretty Good Privacy (PGP) manual (excerpts)

Philip Zimmerman (March 6, 1993)

* Document obtained by CPSR through the Freedom of Information Act

Cryptography and Privacy



Legal and policy
aspects of
information-
technology use and
development.

David Benisar, *Computer Professionals for Social Responsibility*

BATTLE FOR CONTROL OF ENCRYPTION TECHNOLOGY

NOT TOO LONG AGO, MENTIONING ENCRYPTION would evoke visions of James Bond or cereal-box decoder rings. Today, encryption is a very real part of common communication devices like cordless and cellular telephones and local-area networks. Its purpose, not unlike that of the comic-book visions, is to protect the privacy and security of messages and other sensitive information, such as the electronic transfer of money between accounts or contractual agreements done electronically. However, unlike the realm of imagination, the real world, with its conflicting needs, is a threat to the widespread use of this protection device.

OPPOSING CAMPS. There are basically two sides in the conflict for encryption control. In the first camp are law-enforcement and intelligence agencies — the National Security Agency and the FBI — who wish to use wire surveillance as a tool to combat crime, primarily narcotics, but also industrial espionage and anything that threatens national security. The regulatory tools at their disposal include

- ♦ *Export Administration Act.* Authorizes the President to prevent the export of materials and equipment that may be considered harmful to national security if enemy nations use them. It is used primarily to block the export of weapons and other munitions. Encryption is considered a technology with both military and civilian uses, so it is subject to this act.

- ♦ *Patent Secrecy Act.* Lets the government classify pending patents and suppress consumer devices, including encryption devices, to protect national security.

In the second camp are the computer and telephone companies that must comply with any new legal requirements. There is also the general public, who risks losing privacy. Computer Professionals for Social Responsibility — a national membership organization of computing professionals and other interested individuals, based in Palo Alto, California — believes that there should be a new public-encryption standard to protect private communications and that intelligence agencies should not inter-

fere with its creation.

We also believe that there is an inherent conflict of interest when the agency authorized to wire tap is the same agency that defines the system to protect individual privacy. We feel that national interest is better served by promoting privacy-enhancing technologies and the free flow of scientific information.

We base our position on evidence that these agencies are becoming too deeply involved in encryption development. Internal memorandums we obtained from the National Institute of Standards and Technology through the Freedom of Information Act indicate that the NSA is using technical assistance as a way to assume primary control of cryptography development. This is in violation of the Computer Security Act of 1987, which designates NIST as the primary agency

for civilian encryption and limits NSA's involvement in nonmilitary computer security.

Also, companies view these agencies' increased involvement in encryption as a threat to their future:

- ♦ AT&T has repeatedly stated that privacy is an essential part of their business. If people lose trust in that privacy, they may avoid using telephones. It is also expensive to redesign equipment according to new requirements.

- ♦ Other companies fear industrial espionage from foreign companies and governments because the encryption standard the NSA is proposing is too easy to crack.

- ♦ Services companies hope to provide in the future (like electronic voting) will demand absolute confidentiality.

- ♦ Those who wish to export encryption devices must go through a long review process to ensure that the NSA can maintain its surveillance ability. Rather than produce two separate product lines for domestic and export use, most companies simply avoid offering encryption. Those that do can offer only a weak security version authorized by the NSA. Consequently, US companies have lost a market share to foreign companies who can provide more adequate encryption. And the US public has lost its

**THE AGENCY
THAT CONDUCTS
SURVEILLANCE
SHOULDN'T BE
THE ONE THAT
GENERATES AN
ENCRYPTION
STANDARD.**

Editor: George B. Trubow
John Marshall Law School
315 S. Plymouth Ct.
Chicago, IL 60604

assurance of privacy.

Finally, there is some doubt about the effectiveness of wiretapping as a crime-prevention measure. According to data from the US Department of Justice, there were well under 1,000 wiretaps last year, compared to over 140 million installed phone lines and a half trillion phone calls in 1991. Each federal tap cost an average of \$64,000. The length and number of calls per taps have increased three-fold in the last 20 years, but now fewer than 20 percent of all calls recorded are relevant to the police. In fact, arrests due to taps account for only 3,000 of the more than 14 million total arrests made annually.

There is also the history of illegal wiretapping by the NSA and FBI, local government, and private parties. Many states have reported such incidents.

EARLY BATTLES. Obvious efforts to stop the widespread use of encryption date back to the 1970s, when expertise in encryption expanded beyond US intelligence agencies and law-enforcement agencies began to see the need to

assert their control of public encryption.

In 1972, the National Bureau of Standards undertook to create an encryption standard for unclassified information to be used by the government and the public. The NBS made a public call for candidate algorithms and asked the NSA to provide technical support. IBM proposed its Lucifer algorithm, which had a 128-bit key. The NSA reduced the key size to 56 bits, changed the internal workings, and released the modified algorithm as the Data Encryption Standard. Many prominent cryptographers believe that this cut in key size was NSA's attempt to make it easier to crack the DES.

In 1975, NSA officials claimed exclusive control over encryption development and attempted to prevent the National Science Foundation from providing grants to mathematicians who wished to study encryption. The NSF rejected the claim but agreed to let the NSA review the grant proposals strictly for their technical merit.

In 1975, the NSA attempted to use the Patent Secrecy Act to suppress the Phasor-

phone, a \$100 attachment to any telephone that inverts voice frequencies to prevent eavesdropping. When the Phasophone inventor turned to the news media to publicize the action, the NSA quietly rescinded its suppression.

OVERCOMINGS. Despite these battles, the worldwide dissemination of encryption continues—in no small part because it is easy to transfer programs across borders. In addition, many of the leading experts in cryptography live in Europe and Israel, and numerous packages are already available overseas. Cryptos, a \$50 package available on the streets of Moscow, offers full DES and RSA public-key encryption (the box below explains these terms). Another program, Pretty Good Privacy, was created in the US but is available worldwide on Internet and many bulletin boards. The most recent versions of PGP were created in Europe and imported into the US to avoid the strict US export-control laws. (Europe relaxed its export laws on software after the Cold War.)

ENCRYPTION TERMINOLOGY UNSCRAMBLLED

Here are short descriptions of several important terms.

Back door. A secret method built into an encryption system that lets a third party read messages without the key.

Ciphertext. The result of transforming cleartext with an encryption algorithm. Also known as cryptotext.

Cleartext. Unencrypted text. Also known as plaintext. Contrasts to ciphertext, or cryptotext.

Cryptography. The science of transforming a message to make it unintelligible to all but the intended receiver.

Data Encryption Standard. A popular private-key encryption algorithm originally released in 1977 by the US National Bureau of Standards.

Digital signatures. A method for establishing that the message is authentic (not a forgery).

Encryption. The technique of scrambling messages to prevent eavesdropping.

Key. An input that controls the transformation of data by an encryption algorithm.

Private-key encryption. Encryption method in which a single key (symmetric) is used to encrypt and decrypt a message. This method is older than the other popular method, public-key encryption, and was the method used by spies in World War II. This type of encryption demands a prearranged code or master code known by both parties. The advantage is that this type of encryption is not computationally intensive and can even be done by hand.

Pretty Good Privacy. A popular free program that uses the RSA algorithm and is available worldwide.

Public-key encryption. An asymmetric system, based on exponential algorithms, that uses a public key and a private key. Messages sent to the users are encrypted using the public key, which is publicly distributed and decrypted with a private key that the user keeps secret. Examples using this method are digital signatures, electronic contracts (electronic data interchange), and e-mail.

RSA. A popular public-key-encryption algorithm developed by Ron Rivest, Adi Shamir, and Len Adleman of the Massachusetts Institute of Technology. It is based on the factoring two large prime numbers and is computationally impossible to crack without knowing the two members.

CURRENT BATTLES. As encryption becomes a common feature in many programs and consumer products, the FBI and NSA are renewing legislative and administrative efforts to limit further advances.

In 1991, the American National Standards Institute considered a new encryption standard for digital cellular telephones. The NSA felt that the standard would be too difficult to crack and threatened to block exporting of any telephones using that standard. The manufacturers consequently accepted a standard that was vulnerable to cracking by any skilled PC user. In contrast, when Australian law-enforcement agencies made a similar request in 1993, the Australian government rejected it, ultimately approving a more secure standard, even though law-enforcement agencies might not be able to crack it.

Also in 1991, the FBI asked US Senator Joseph Biden (D-Delaware) to introduce a nonbinding resolution recommending that, given lawful authorization, telephone companies would unscramble messages for law-enforcement officials. Opposition from industry and civil-liberties groups, which argued that the proposal would limit the development and dissemination of encryption, led to the resolution's withdrawal.

In March 1992, the FBI went back to the Judiciary Committee with a proposal that would require all providers and manufacturers of telecommunications services to redesign communications equipment to meet a standard that was to be considered in closed hearings. To minimize publicity, the FBI tried to have the proposal inserted into an existing bill (which later became the FCC Reauthorization Act) and designate the Federal Communications Commission as the lead agency in setting technical requirements for compliance. Providers could be fined up to \$10,000 per day for noncompliance, and although they would have only 180 days to redesign and install the new systems, they would be allowed to recoup costs by increasing their rates. Needless to say, the scheme generated controversy and was never formally introduced.

In May 1992, the FBI returned with a new version of the March proposal that gave the Attorney General the authority to monitor and approve or reject all telecommunications equipment. The proposal mandated that "all communications providers supply the government with the ability to intercept wire and electronic communications concurrent with the transmission...at a government monitoring facility remote from the target facility and the system of the electronic communications services provider...within 18 months." Although penalties remained at \$10,000 per day for noncompliance, there was no mention in this version of how to recoup system-redesign costs.

The CPSR used the Freedom of Information Act to request documents from all involved government agencies summarizing the May proposal's expected effect. The documents revealed that there was considerable debate inside the government about the proposal's utility. The General Services Administration, the chief communications-equipment procurement agency of the US government, even described the proposal as a threat to national security:

The proposed legislation would... make it easier for criminals, terrorists, foreign intelligence (spies), and computer hackers to electronically penetrate the public network and pry into areas previously not open to snooping.

The General Accounting Office also found problems:

[N]either the FBI nor the telecommunications industry has

systematically identified the alternatives, or evaluated their costs, benefits, or feasibility....

Because of the proposal's controversial nature and strong opposition, no senator or congressman was willing to sponsor it, but the general expectation is that the FBI will try to propose it again.

In the most recent development to limit the dissemination of encryption technology, the White House announced on April 16, 1993, the NSA's development of the Clipper chip, whose classified inner workings and algorithm could become a standard for all computers, telephones, and fax machines and a requirement for all government contractors who deal with unclassified, sensitive information. Although it does provide some communications security, the chip has a significant security flaw. The Attorney General designates two trusted escrow agents, one of whom is a member of a government agency, to hold the key that unscrambles the owner's messages. The two escrow agents give the key to government officials when presented with a court order. Consequently, the user must depend on these agents to keep the keys secure. As cryptographer Whitfield Diffie notes, this creates a front door, not a back door, to the system.

The White House is reviewing the US government's encryption policy, but the directive ordering this review is not available to the public. On May 29, 1993, the CPSR filed suit against the NSA to force disclosure of how the Clipper chip will function and the language of the policy directive.

THE BATTLE CONTINUES. Intelligence and law-enforcement agencies will continue to fail at stopping the development of encryption, as long as people recognize that these technologies are essential to maintaining private and secure communications. As practitioners, there are several things you can do.

- ♦ Incorporate privacy- and security-enhancing technologies into your products.
- ♦ Advise those that purchase equipment for your company to avoid devices such as the Clipper chip, which may compromise your security and that of your clients.
- ♦ Get involved. Contact your Congressional representative and senators at (202) 224-3121 and tell them what you think of these proposals. ♦

USA

Marc Rotenberg

The only locksmith in town

The NSA's efforts to control the dissemination of cryptography

In August 1989, the National Security Agency (NSA), a secret intelligence organisation in the United States, attempted to suppress the dissemination of an article written by Ralph C. Merkle, a computer scientist at Xerox's research center in California, in which he showed how to protect, cheaply and effectively, the privacy and security of computer communications. It was only the most recent incident in a long history of NSA efforts to limit public knowledge of innovations in cryptography.

The National Security Agency was created in 1952 by a presidential memorandum that is still classified. It has operated since that time under a series of presidential orders, outside the normal channels of government accountability. The NSA's secrecy is legendary: it has no legislative charter and its existence was not even acknowledged until 1962; no director of the agency appeared in an open hearing of Congress until 1975, and its budget, though in excess of several billion dollars, is secret and not known to many members of Congress.

The NSA is charged with safeguarding classified communications for the United States government around the world. But it is also engaged in collecting computer communications and telephone signals, cracking communications locks throughout the world, and gathering intelligence. It is of particular interest to computer scientists because of its extraordinary computational resources (several Cray supercomputers have been installed at Fort Meade outside Washington, DC) and because of its classified research in signal processing and data encryption.

President Reagan tried to expand the NSA's authority when he signed a National Security Decision Directive on 17 September 1984 which gave the NSA authority over computer and communications security for the entire government. (Previously, the National Bureau of Standards (NBS), a civilian agency, had been responsible for computer security for other civilian agencies in the federal government.) Congress responded by passing the Computer Security Act, a law meant to reestablish civilian

control over computer security. But a memorandum of understanding signed recently by the NSA and the National Institute of Standards and Technology (successor to the NBS) calls into question whether the Act will be implemented as Congress intended.

Still, the NSA continues its efforts to control the flow of research on data encryption, and for good reason. As countries become increasingly dependent on computer communications, the need to ensure the privacy and security of messages that travel along computer networks grows, and computer scientists are particularly aware of the vulnerability of these communications. Data encryption is the most important technical safeguard for ensuring the privacy and security of these messages, but the NSA has repeatedly used funding restrictions and outright censorship to try to control the publication of cryptography research and to limit public access in this way.

In 1975, the NSA warned the National Science Foundation, the primary funding authority for scientific research in the US, against funding cryptography research, claiming that the NSA had sole authority to conduct such research. The agency continued to use strong-arm tactics in subsequent years to discourage unclassified research on data encryption.

When the NSA's efforts to control funding proved insufficient to restrict this research, a system of voluntary submission of materials by cryptography researchers was established, often with consent from the academic community. George Davida, a computer scientist at the University of Wisconsin and a member of the special committee of the American Council for Education that recommended submission of research to the NSA, opposed the plan.

In David Burnham's book, *The Rise of the Computer State*, Dr Davida describes how the rapid computerization of information has created electronic windows that make it possible to peer into the 'most intimate details of people's lives'. The databases become one-way mirrors, and encryption is often the only way to create a curtain to shield information from intruders. Dr Davida warns that 'the need for a civilian (or nongovernmental) effort in cryptography is a strong one'.

Despite these sorts of efforts, the NSA recently lost its battle to decertify DES, a widely-used encryption procedure that

allows the parties involved in the communication to control the encryption scheme. The NSA had proposed a proprietary technology that would have required the use of cryptography keys developed by the NSA. But US businesses, particularly the Bankers' Association, successfully opposed this, fearing that it would grant the NSA the ability to examine computer communications, regardless of national security interest.

The NSA contends that it must retain the capacity to decrypt any communication in the world to protect national security. But at the heart of the debate over the agency's role in cryptography research is whether it should be the only locksmith in town. Fifteen years ago, when the US Select Committee on Intelligence conducted hearings on the activities of intelligence agencies, Senator Frank Church, the chairman of the committee, agreed that the NSA's intelligence-gathering capabilities were essential to the country's security, but warned that the eavesdropping devices and computers of the NSA created 'tremendous potential for abuse'.

A 1987 report prepared by Congress's Office of Technology Assessment (OTA) was similarly critical of giving the NSA sole control. Though OTA noted that the 'NSA sees its signal intelligence mission to be at risk if effective cryptography were available worldwide', the report also found that the United States can no longer base its cryptography policy on the interests of the national security community because of challenges in technology, 'continued pressure to improve business and government operations', and the 'emerging internalization' of encryption technology.

Computer Professionals for Social Responsibility, a non-partisan national membership organisation, has recommended that Congress conduct open hearings on cryptography research and explore the impact of the NSA's efforts to restrict public access to new developments in the field. With the growing dependence of computer users on digitized transmission, data encryption and the policies controlling it become all the more important. ■

Marc Rotenberg, *Testimony before the Subcommittee on Legislation and National Security, Committee on Government Operations, US House of Representatives on the Computer Security Act of 1987, May 4, 1989.*

Marc Rotenberg is the Director of the Washington Office of Computer Professionals for Social Responsibility and former Counsel to the Senate Judiciary Committee.

"Proposed Privacy Guidelines for the NREN"

Statement of Marc Rotenberg,
Washington Director
Computer Professionals for Social Responsibility (CPSR)

Open Forum on Library and Information Service's Roles in the
National Research and Education Network (NREN)

National Commission on Libraries and
Information Science (NCLIS)
Washington, DC
July 21, 1992

Thank you for the opportunity to testify today before the National Commission on Library and Information Science (NCLIS). My name is Marc Rotenberg and I am the Director of the Washington Office of Computer Professionals for Social Responsibility (CPSR). CPSR is a national organization of professionals in the computing field.

I would like to speak with you about privacy protection and the future of the NREN. This is item 6 identified in the NREN research agenda. Richard Civile will speak with you next about CPSR's work to promote Local Civic Networks.

During the past few years CPSR has coordinated several national efforts to promote privacy protection for network communication. From cryptography to Caller ID, we have sought to ensure that the rapid developments in the communications infrastructure do not diminish the privacy we all value. We believe that the future of network communications depends largely on the ability to make certain that sufficient privacy protection is available for all users of the network.

In this effort we have worked closely with the library community. It became clear to us that library organizations have a special appreciation for the importance of privacy protection. For many, privacy is the critical safeguard that protects intellectual freedom and promotes the open exchange of information. The American Library Association, the Association of Research and other library organizations have all shown their support for privacy protection through codes of conduct, policy statements, and research conferences.

We have also worked closely with telecommunication policy makers in the United States and around the world. The New York state Public Service Commission issued a policy on telecommunication privacy which set out several principles for network communications. These recommendations have been followed

in several states. More recently, the Minister of Communications in Canada issued a series of principles on communications policy. Meanwhile, the Commission of the European Communities has put forward a draft directive on Data Protection in Telecommunications.

The European Commission made a critical point about future network development. It said that "the effective protection of personal data and privacy is developing into an essential precondition for social acceptance of new digital networks and services." This view is shared by agencies in other countries that have looked at the implications of advanced networking services. For example, the Ministry of Posts and Telecommunications in Japan recently concluded a study on the protection of personal data in the telecommunications business and recommended a series of privacy guidelines to accompany the introduction of new network services.

In the United States, however, we find ourselves in the midst of the greatest privacy debate in a generation. In the absence of a coherent federal policy to protect privacy, consumers have been left to fend for themselves, and the response is not encouraging. From Pennsylvania to California, telephone companies now face widespread and well-founded consumer opposition to new telephone services. Part of the reason for this is that there has been little effort in the United States at the federal level to develop privacy principles for new network services.

CPSR would like to see an agency in the United States take on the task of developing and promulgating privacy principles for network services. We have already recommended the creation of a data protection board which could, among other tasks, develop appropriate principles for network communications. There is a proposal before Congress to establish such an agency, but is unclear whether it will be enacted this year.

Meanwhile, the Federal Communications Commission (FCC) has been unwilling to address the privacy implications of new network services. We are also somewhat disappointed that neither the Computer Science and Technology Board (CSTB) of the National Research Council or the Office of Technology Assessment (OTA) has addressed privacy concerns for network users. Both the CSTB and the OTA are well qualified to tackle this problem.

In the interim, NCLIS could take a leadership role, and help develop and promulgate privacy principles for the emerging communications infrastructure. It is clearly in the interest of the library and information science community to ensure adequate privacy protection, but unless some agency takes on this responsibility it appears unlikely that the work will be undertaken.

CPSR believes that it is in the long-term interest of our country and of computer users around the world to ensure

protection for networked communication. The failure to develop such policy may impose very high costs on all network users, and may ultimately reduce greatly the value of the network to users.

Speaking academically, the absence of adequate protection for electronic communication is a substantial gap in NREN policy that should soon be addressed if the full potential of the infrastructure is to be realized. Speaking practically, if we don't get some good policy soon, we may all be buried in a blizzard of electronic junkmail the likes of which we have never known.

I would like now to make three points about the current state of privacy protection for NREN, and then propose a series of principles for privacy protection. These principles may help "get the ball rolling" and encourage the development of other initiatives. I hope that NCLIS will recommend that the Office of Science and Technology Policy (OSTP) give these principles full consideration.

FINDING 1:

Commercialization of the NREN will exacerbate existing privacy problems. Without a clear mechanism to protect privacy, user concerns will increase.

Much of the discussion surrounding the NREN today focuses on the opportunity to develop commercial services and to provide network access for private carriers. We do not oppose efforts to provide commercial services. Clearly, there is an important opportunity to develop new services and to offer products through the network. At the same time, it is apparent that the commercialization of the NREN will create new pressures on privacy protection.

In the current network environment, made up primarily of researchers and scientists, there is little incentive or opportunity to gather personal data, to compile lists, or to sell personal information. This is likely to change. Once commercial transactions begin to take place on the net, the information environment will resemble a hybrid of credit card and telephone call transactions. Records of individual purchases will be available and will possess commercial value. The NREN community will face a whole new set of privacy issues.

We anticipate that there will be three different types of privacy problems as the NREN continues to evolve. First, as commercial organizations become users of the network, they will gather personal data, and wish to sell lists. The address files for list servers could be sold, and users may find themselves "subscribed" to lists they have no interest in. These activities will raise traditional privacy concerns about the restrictions on

disclosure and secondary use, the opportunity for users to obtain information held by others, and the need to minimize the collection of personal information.

Second, efforts to promote competitiveness in the delivery of network services may also lead to the disclosure of network data which will compromise user privacy.

This problem is already apparent in the current rules for the operation of the telephone network. The Federal Communication Commission requires telephone companies to provide records of customer phone calls to other companies so that competing companies may analyze calling patterns and sell their services. Large companies objected to the disclosure of this sensitive information. As a result the FCC required that telephone companies obtain authorization before releasing these numbers. But this restriction only applies to telephone customers with more than 20 lines.

The disclosure of Customer Proprietary Network Information (CPNI) has already surprised many telephone customers who now receive calls from companies with whom they have no prior relationship. These companies are able to describe the customer's telephone calling habits in great detail. Users of NREN services are also likely to object to the disclosure of network information.

The third problem is that law enforcement agencies are likely to make "greater demands" on communication service providers to turn over records of electronic communications to the government and to provide assistance in the execution of warrants. I say "greater demands" with some reservation since the recent proposal from the Federal Bureau of Investigation to require that all communications equipment in the United States be capable of wiretapping seems about the greatest demand conceivable. Still, we should anticipate that the government demands for access to the contents and records of NREN communications are likely to increase.

FINDING 2:

Current privacy protections are inadequate

Electronic communications are provided some protection against unlawful interception by the Electronic Communications Privacy Act (ECPA) of 1986. This law extends the very important guarantees contained within the 1968 wiretap statute to digital communication and stored electronic mail. But this protection now appears inadequate. As a general matter, the wiretap law protects the contents of an electronic message against unlawful disclosure; it does not protect the record of the transaction against disclosure.

ECPA also does not appear to protect critical personal information, such as a person's telephone number, from improper disclosure. For example, the Calling Number Identification (CNID) service is probably a violation of the wiretap statute and clearly a violation of the wiretap law of several states. Nonetheless, the service has been offered over the objection of consumer groups, technical experts, and legal scholars.

FINDING 3:

Technical safeguards provide only a partial solution

There are some in the network community who believe that technology will provide a solution to these emerging privacy problems. New techniques in cryptography provide ways to protect the contents of an electronic message and even to protect the identity of the message author. An article that will appear next month in Scientific American titled "Achieving Electronic Privacy" describes in more detail how it may be possible through technical means to recapture some privacy.

CPSR has supported many efforts to improve technical means for privacy protection. In fact, CPSR has been of the leading proponents of the widespread use of cryptography to protect electronic communications. We have opposed restrictions by both the National Security Agency and the Federal Bureau of Investigation on the use of cryptography. We have also supported the development of privacy-enhancing technologies, such as telephone cards which are widely used in Europe and Japan, and recommended that policy makers explore technical means to protect information.

Nonetheless, we do not believe that technical safeguards will provide sufficient protection for networked communications. Our right of privacy is based on Constitutional principles and our national history, and reflects our commitment to certain political ideals. The protection of privacy is ultimately a policy decision that must be resolved through our political institutions. Clearly, technology provides useful developments that we should incorporate into future networks, but it would be a mistake to assume that technology alone will provide sufficient protection.

This point was made two decades ago by former White House Science Adviser Jerome Wiesner who also served as president of MIT. In testimony before Congress on the privacy implications of databanks, Professor Wiesner said:

"There are those who hope new technology can redress these invasions of personal autonomy that information technology now makes possible, but I don't share this hope. To be sure, it is possible and desirable to provide technical safeguards against unauthorized access. It is even conceivable that computers could be programmed to have their memories fade with time and to eliminate specific identity. Such safeguards are highly desirable, but the basic safeguards cannot be provided by new inventions. They must be provided by the legislative and legal systems of this country. We must face the need to provide adequate guarantees for individual privacy."

We believe that the development of NREN privacy policy should be conducted in this spirit: looking for opportunities to incorporate technical safeguards while recognizing that the ultimate decisions are policy-based.

PRIVACY GUIDELINES

Before discussing the proposed privacy principles, I would like to say a few words about the desirability of developing these principles. Privacy protection in electronic environments is a particularly complex policy problem. There is legal jargon and technical jargon. There are rapid changes. And there are certainly a wide range of opinions about how best to achieve privacy, even about what privacy means.

Privacy principles have helped to clarify goals and to convey objectives in non-technical terms. Well developed policies are "technology neutral" and are adaptable as new technologies emerge. Professional organizations have made widespread use of such principles for codes of ethics and for public education.

There are a number of such policies in the privacy realm. Some of these policies have been extremely influential in the development of public policy, national law, and international agreements. For example, the Code of Fair Information Practices was the basis for the Privacy Act of 1974, the most extensive privacy law in the United States. The Code was developed by a special task force created by the Secretary of Health, Education, and Welfare in 1973. Other codes have formed the basis for data protection law in Great Britain.

All of these codes seek to establish certain responsibilities for organizations that collect personal information, and to create certain rights for individuals.

In developing these telecommunication privacy guidelines, we examined existing codes and particularly the principles developed

by the Organization for Economic and Cooperative Development (OECD) in 1981. We also incorporated several additional principles that we believe are necessary to protect personal information in communication environments.

Taken as a whole, the principles are intended to improve privacy protection for network communications as the NREN continues to evolve.

RECOMMENDATION 1:

The confidentiality of electronic communications should be protected.

The primary purpose of a communication network is to ensure that information can travel between two points without alteration, interception, or disclosure. A network that fails to achieve this goal will not serve as a reliable conduit for information. Therefore the primary goal should be to guarantee the confidentiality of electronic communications.

RECOMMENDATION 2:

Privacy considerations must be recognized explicitly in the provision, use and regulation of telecommunication services.

The addition of new services to a communications infrastructure will necessarily raise privacy concerns. Users should be fully informed about the privacy implications of these services so that they are able to make appropriate decisions about the use of services.

RECOMMENDATION 3:

The collection of personal data for telecommunication services should be limited to the extent necessary to provide the service.

Users should not be required to disclose personal data which is not necessary for the rendering of the service. In particular, the use of the Social Security number should be avoided. In no instance, should it be used as both an identifier and authenticator.

RECOMMENDATION 4:

Service providers should not disclose information without the explicit consent of service users. Service providers should be required to make known their data collection practices to service users.

Service providers have a responsibility to inform users about the collection of personal information and to protect the information against unlawful disclosure. Personally identifiable information should not be disclosed without the affirmative consent of the user.

RECOMMENDATION 5:

Users should not be required to pay for routine privacy protection. Additional costs for privacy should only be imposed for extraordinary protection.

The premise of the federal wiretap statute is that all users of the public network are entitled to the same degree of legal protection against the unlawful disclosure of electronic communications. This principle should be carried forward into the emerging network environment. Segmented levels of privacy protection are also likely to introduce new transaction costs and create inefficiencies. Where special charges are imposed for privacy, it should be for "armored car" service.

RECOMMENDATION 6:

Service providers should be encouraged to explore technical means to protect privacy.

Service providers should pursue technical means to protect privacy, particularly where such means may improve the delivery of service and reduce the risk of privacy loss.

RECOMMENDATION 7:

Appropriate security policies should be developed to protect network communications

Security is an element of privacy protection but it is not synonymous with privacy protection. Appropriate security policies should be put in place to protect privacy. However, it should be recognized that some security measures may compromise privacy protection. Network monitoring, for example, or the collection of detailed audit trail information will raise substantial privacy

concerns. Therefore, security policies should be designed to serve the larger goal of privacy protection.

RECOMMENDATION 8:

A mechanism should be established to ensure the observance of these principles.

Good principles without appropriate oversight and enforcement are insufficient to protect privacy. This has been the experience of the United States with the Privacy Act of 1974 and of the European countries with the OECD principles of 1981. In both instances, fine principles lacked sufficient oversight and enforcement mechanisms.

Additional principles may be appropriate and these principles may well need modification. But we hope that they will provide a good starting point for a discussion on communications privacy for the NREN.

[Attachments: "Protecting Privacy," Communications of the ACM, April 1992; "Communications Privacy: Implications for Network Design," Proceedings of INET '92, Kobe, Japan)]

The Impact of a Secret Cryptographic Standard
on Encryption, Privacy, Law Enforcement
and Technology

Whitfield Diffie
Sun Microsystems
11 May 1993

I'd like to begin by expressing my thanks to Congressman Boucher, the other members of the committee, and the committee staff for giving us the opportunity to appear before the committee and express our views.

On Friday, the 16th of April, a sweeping new proposal for both the promotion and control of cryptography was made public on the front page of the New York Times and in press releases from the White House and other organizations.

This proposal was to adopt a new cryptographic system as a federal standard, but at the same time to keep the system's functioning secret. The standard would call for the use of a tamper resistant chip, called Clipper, and embody a 'back door' that will allow the government to decrypt the traffic for law enforcement and national security purposes.

So far, available information about the chip is minimal and to some extent contradictory, but the essence appears to be this: When a Clipper chip prepares to encrypt a message, it generates a short preliminary signal rather candidly entitled the Law Enforcement Exploitation Field. Before another Clipper chip will decrypt the message, this signal must be fed into it. The Law Enforcement Exploitation Field or LEEF is tied to the key in use and the two must match for decryption to be successful. The LEEF in turn, when decrypted by a government held key that is unique to the chip, will reveal the key used to encrypt the message.

The effect is very much like that of the little keyhole in the back of the combination locks used on the lockers of school children. The children open the locks with the combinations, which is supposed to keep the other children out, but the teachers can always look in the lockers by using the key.

In the month that has elapsed since the announcement, we have studied the Clipper chip proposal as carefully as the available information permits. We conclude that such a proposal is at best premature and at worst will have a damaging effect on both business security and civil rights without making any improvement in law enforcement.

To give you some idea of the importance of the issues this raises, I'd like to suggest that you think about what are the most essential security mechanisms in your daily life and work. I believe you will realize that the most important things any of you ever do by way of security have nothing to do with guards, fences, badges, or safes. Far and away the most important element of your security is that you recognize your family, your friends, and your colleagues. Probably second to that is that you sign your signature, which provides the people to whom you

give letters, checks, or documents, with a way of proving to third parties that you have said or promised something. Finally you engage in private conversations, saying things to your loved ones, your friends, or your staff that you do not wish to be overheard by anyone else.

These three mechanisms lean heavily on the physical: face to face contact between people or the exchange of written messages. At this moment in history, however, we are transferring our medium of social interaction from the physical to the electronic at a pace limited only by the development of our technology. Many of us spend half the day on the telephone talking to people we may visit in person at most a few times a year and the other half exchanging electronic mail with people we never meet in person.

Communication security has traditionally been seen as an arcane security technology of real concern only to the military and perhaps the banks and oil companies. Viewed in light of the observations above, however, it is revealed as nothing less than the transplantation of fundamental social mechanisms from the world of face to face meetings and pen and ink communication into a world of electronic mail, video conferences, electronic funds transfers, electronic data interchange, and, in the not too distant future, digital money and electronic voting.

No right of private conversation was enumerated in the constitution. I don't suppose it occurred to anyone at the time that it could be prevented. Now, however, we are on the verge of a world in which electronic communication is both so good and so inexpensive that intimate business and personal relationships will flourish between parties who can at most occasionally afford the luxury of traveling to visit each other. If we do not accept the right of these people to protect the privacy of their communication, we take a long step in the direction of a world in which privacy will belong only to the rich.

The import of this is clear: The decisions we make about communication security today will determine the kind of society we live in tomorrow.

The objective of the administration's proposal can be simply stated:

They want to provide a high level of security to their friends, while being sure that the equipment cannot be used to prevent them from spying on their enemies.

Within a command society like the military, a mechanism of this sort that allows soldiers' communications to be protected from the enemy, but not necessarily from the Inspector General, is an entirely natural objective. Its imposition on a free society, however, is quite another matter.

Let us begin by examining the monitoring requirement and ask both whether it is essential to future law enforcement and what measures would be required to make it work as planned.

Eavesdropping, as its name reminds us, is not a new phenomenon. But in spite of the fact that police and spies have been doing it for a long time, it has acquired a whole new dimension since

the invention of the telegraph. Prior to electronic communication, it was a hit or miss affair. Postal services as we know them today are a fairly new phenomenon and messages were carried by a variety of couriers, travelers, and merchants. Sensitive messages in particular, did not necessarily go by standardized channels. Paul Revere, who is generally remembered for only one short ride, was the American Revolution's courier, traveling routinely from Boston to Philadelphia with his saddle bags full of political broadsides.

Even when a letter was intercepted, opened, and read, there was no guarantee, despite some people's great skill with flaps and seals, that the victim would not notice the intrusion.

The development of the telephone, telegraph, and radio have given the spies a systematic way of intercepting messages. The telephone provides a means of communication so effective and convenient that even people who are aware of the danger routinely put aside their caution and use it to convey sensitive information. Digital switching has helped eavesdroppers immensely in automating their activities and made it possible for them to do their listening a long way from the target with negligible chance of detection.

Police work was not born with the invention of wiretapping and at present the significance of wiretaps as an investigative tool is quite limited. Even if their phone calls were perfectly secure, criminals would still be vulnerable to bugs in their offices, body wires on agents, betrayal by co-conspirators who saw a brighter future in cooperating with the police, and ordinary forensic inquiry.

Moreover, cryptography, even without intentional back doors, will no more guarantee that a criminal's communications are secure than the Enigma guaranteed that German communications were secure in World War II. Traditionally, the richest source of success in communications intelligence is the ubiquity of busts: failures to use the equipment correctly.

Even if the best cryptographic equipment we know how to build is available to them, criminal communications will only be secure to the degree that the criminals energetically pursue that goal. The question thus becomes, "If criminals energetically pursue secure communications, will a government standard with a built in inspection port, stop them.

It goes without saying that unless unapproved cryptography is outlawed, and probably even if it is, users bent on not having their communications read by the state will implement their own encryption. If this requires them to forgo a broad variety of approved products, it will be an expensive route taken only by the dedicated, but this sacrifice does not appear to be necessary.

The law enforcement function of the Clipper system, as it has been described, is not difficult to bypass. Users who have faith in the secret Skipjack algorithm and merely want to protect themselves from compromise via the Law Enforcement Exploitation Field, need only encrypt that one item at the start of transmission. In many systems, this would require very small changes to supporting programs already present. This makes it likely that if Clipper chips become as freely available as has been suggested, many products will employ them in ways that defeat a major objective of the plan.

What then is the alternative? In order to guarantee that the government can always read Clipper traffic when it feels the need, the construction of equipment will have to be carefully controlled to prevent non-conforming implementations. A major incentive that has been cited for industry to implement products using the new standard is that these will be required for communication with the government. If this strategy is successful, it is a club that few manufacturers will be able to resist. The program therefore threatens to bring communications manufacturers under an all encompassing regulatory regime.

It is noteworthy that such a regime already exists to govern the manufacture of equipment designed to protect 'unclassified but sensitive' government information, the application for which Clipper is to be mandated. The program, called the Type II Commercial COMSEC Endorsement Program, requires facility clearances, memoranda of agreement with NSA, and access to secret 'Functional Security Requirements Specifications.' Under this program member companies submit designs to NSA and refine them in an iterative process before they are approved for manufacture.

The rationale for this onerous procedure has always been, and with much justification, that even though these manufacturers build equipment around approved tamper resistant modules analogous to the Clipper chip, the equipment must be carefully vetted to assure that it provides adequate security. One requirement that would likely be imposed on conforming Clipper applications is that they offer no alternative or additional encryption mechanisms.

Beyond the damaging effects that such regulation would have on innovation in the communications and computer industries, we must also consider the fact that the public cryptographic community has been the principal source of innovation in cryptography. Despite NSA's undocumented claim to have discovered public key cryptography, evidence suggests that, although they may have been aware of the mathematics, they entirely failed to understand the significance. The fact that public key is now widely used in government as well as commercial cryptographic equipment is a consequence of the public community being there to show the way.

Farsightedness continues to characterize public research in cryptography, with steady progress toward acceptable schemes for digital money, electronic voting, distributed contract negotiation, and other elements of the computer mediated infrastructure of the future.

Even in the absence of a draconian regulatory framework, the effect of a secret standard, available only in a tamper resistant chip, will be a profound increase in the prices of many computing devices. Cryptography is often embodied in microcode, mingled on chips with other functions, or implemented in dedicated, but standard, microprocessors at a tiny fraction of the tens of dollars per chip that Clipper is predicted to cost.

What will be the effect of giving one or a small number of companies a monopoly on tamper resistant parts? Will there come a time, as occurred with DES, when NSA wants the standard changed even though industry still finds it adequate for many applications? If that occurs will industry have any recourse but to do what it is told? And who will pay for the conversion?

One of the little noticed aspects of this proposal is the arrival of tamper resistant chips in the commercial arena. Is this tamper resistant part merely the precursor to many? Will the open competition to improve semiconductor computing that has characterized the past twenty-years give way to an era of trade secrecy? Is it perhaps tamper resistance technology rather than cryptography that should be regulated?

Recent years have seen a succession of technological developments that diminish the privacy available to the individual. Cameras watch us in the stores, x-ray machines search us at the airport, magnetometers look to see that we are not stealing from the merchants, and databases record our actions and transactions. Among the gems of this invasion is the British Rafter technology that enables observers to determine what station a radio or TV is receiving. Except for the continuing but ineffectual controversy surrounding databases, these technologies flourish without so much as talk of regulation.

Cryptography is perhaps alone in its promise to give us more privacy rather than less, but here we are told that we should forgo this technical benefit and accept a solution in which the government will retain the power to intercept our ever more valuable and intimate communications and will allow that power to be limited only by policy.

In discussion of the FBI's Digital Telephony Proposal — which would have required communication providers, at great expense to themselves, to build eavesdropping into their switches — it was continually emphasized that wiretaps were an exceptional investigative measure only authorized when other measures had failed. Absent was any sense that were the country to make the proposed quarter billion dollar investment in intercept equipment, courts could hardly fail to accept the police argument that a wiretap would save the people thousands of dollars over other options. As Don Cotter, at one time director of Sandia National Laboratories, said in respect to military strategy: "Hardware makes policy."

Law, technology, and economics are three central elements of society that must all be kept in harmony if freedom is to be secure. An essential element of that freedom is the right to privacy, a right that cannot be expected to stand against unremitting technological attack. Where technology has the capacity to support individual rights, we must enlist that support rather than rejecting it on the grounds that rights can be abused by criminals. If we put the desires of the police ahead of the rights of the citizens often enough, we will shortly find that we are living in police state. We must instead assure that the rights recognized by law are supported rather than undermined by technology.

At NSA they believe in something they call 'security in depth.' Their most valuable secret may lie encrypted on a tamper resistant chip, inside a safe, within a locked office, in a guarded building, surrounded by barbed wire, on a military base. I submit to you that the most valuable secret in the world is the secret of democracy; that technology and policy should go hand in hand in guarding that secret; that it must be protected by security in depth.

Recommendations

There is a crying need for improved security in American communication and computing equipment and the Administration is largely correct when it blames the problem on a lack of standards. One essential standard that is missing is a more secure conventional algorithm to replace DES, an area of cryptography in which NSA's expertise is probably second to none.

I urge the committee to take what is good in the Administration's proposal and reject what is bad.

- o The Skipjack algorithm and every other aspect of this proposal should be made public, not only to expose them to public scrutiny but to guarantee that once made available as standards they will not be prematurely withdrawn. Configuration control techniques pioneered by the public community can be used to verify that some pieces of equipment conform to government standards stricter than the commercial where that is appropriate.
- o I likewise urge the committee to recognize that the right to private conversation must not be sacrificed as we move into a telecommunicated world and reject the Law Enforcement Exploitation Function and the draconian regulation that would necessarily come with it.
- o I further urge the committee to press the Administration to accept the need for a sound international security technology appropriate to the increasingly international character of the world's economy.

A Cypherpunk's Manifesto

by Eric Hughes

Privacy is necessary for an open society in the electronic age. Privacy is not secrecy. A private matter is something one doesn't want the whole world to know, but a secret matter is something one doesn't want anybody to know. Privacy is the power to selectively reveal oneself to the world.

If two parties have some sort of dealings, then each has a memory of their interaction. Each party can speak about their own memory of this; how could anyone prevent it? One could pass laws against it, but the freedom of speech, even more than privacy, is fundamental to an open society; we seek not to restrict any speech at all. If many parties speak together in the same forum, each can speak to all the others and aggregate together knowledge about individuals and other parties. The power of electronic communications has enabled such group speech, and it will not go away merely because we might want it to.

Since we desire privacy, we must ensure that each party to a transaction have knowledge only of that which is directly necessary for that transaction. Since any information can be spoken of, we must ensure that we reveal as little as possible. In most cases personal identity is not salient. When I purchase a magazine at a store and hand cash to the clerk, there is no need to know who I am. When I ask my electronic mail provider to send and receive messages, my provider need not know to whom I am speaking or what I am saying or what others are saying to me; my provider only need know how to get the message there and how much I owe them in fees. When my identity is revealed by the underlying mechanism of the transaction, I have no privacy. I cannot here selectively reveal myself; I must always reveal myself.

Therefore, privacy in an open society requires anonymous transaction systems. Until now, cash has been the primary such system. An anonymous transaction system is not a secret transaction system. An anonymous system empowers individuals to reveal their identity when desired and only when desired; this is the essence of privacy.

Privacy in an open society also requires cryptography. If I say something, I want it heard only by those for whom I intend it. If the content of my speech is available to the world, I have no privacy. To encrypt is to indicate the desire for privacy, and to encrypt with weak cryptography is to indicate not too much desire for privacy. Furthermore, to reveal one's identity with assurance when the default is anonymity requires the cryptographic signature.

We cannot expect governments, corporations, or other large, faceless organizations to grant us privacy out of their beneficence. It is to their advantage to speak of us, and we should expect that they will speak. To try to prevent their speech is to fight against the realities of information. Information does not just want to be free, it longs to be free. Information expands to fill the available storage space. Information is Rumor's younger, stronger cousin; Information is fleetier of foot, has more eyes, knows more, and understands less than Rumor.

We must defend our own privacy if we expect to have any. We must come together and create systems which allow anonymous transactions to take place. People have been defending their own privacy for centuries with whispers, darkness, envelopes, closed doors, secret handshakes, and couriers. The technologies of the past did not allow for strong privacy, but electronic technologies do.

We the Cypherpunks are dedicated to building anonymous systems. We are defending our privacy with cryptography, with anonymous mail forwarding systems, with digital signatures, and with electronic money.

Cypherpunks write code. We know that someone has to write software to defend privacy, and since we can't get privacy unless we all do, we're going to write it. We publish our code so that our fellow Cypherpunks may practice and play with it. Our code is free for all to use, worldwide. We don't much care if you don't approve of the software we write. We know that software can't be destroyed and that a widely dispersed system can't be shut down.

Cypherpunks deplore regulations on cryptography, for encryption is fundamentally a private act. The act of encryption, in fact, removes information from the public realm. Even laws against cryptography reach only so far as a nation's border and the arm of its violence. Cryptography will ineluctably spread over the whole globe, and with it the anonymous transactions systems that it makes possible.

For privacy to be widespread it must be part of a social contract. People must come and together deploy these systems for the common good. Privacy only extends so far as the cooperation of one's fellows in society. We the Cypherpunks seek your questions and your concerns and hope we may engage you so that we do not deceive ourselves. We will not, however, be moved out of our course because some may disagree with our goals.

The Cypherpunks are actively engaged in making the networks safer for privacy. Let us proceed together apace.

Onward.

Eric Hughes
<hughes@soda.berkeley.edu>

9 March 1993

Computer Security Act

COMPUTER SECURITY ACT OF 1987

For Legislative History of Act, see p. 3120.

An Act to provide for a computer standards program within the National Bureau of Standards, to provide for Government-wide computer security, and to provide for the training in security matters of persons who are involved in the management, operation, and use of Federal computer systems, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the "Computer Security Act of 1987".

SEC. 2. PURPOSE.

(a) **IN GENERAL.**—The Congress declares that improving the security and privacy of sensitive information in Federal computer systems is in the public interest, and hereby creates a means for establishing minimum acceptable security practices for such systems, without limiting the scope of security measures already planned or in use.

(b) **SPECIFIC PURPOSES.**—The purposes of this Act are—

(1) by amending the Act of March 3, 1901, to assign to the National Bureau of Standards responsibility for developing standards and guidelines for Federal computer systems, including responsibility for developing standards and guidelines needed to assure the cost-effective security and privacy of sensitive information in Federal computer systems, drawing on the technical advice and assistance (including work products) of the National Security Agency, where appropriate;

(2) to provide for promulgation of such standards and guidelines by amending section 111(d) of the Federal Property and Administrative Services Act of 1949;

(3) to require establishment of security plans by all operators of Federal computer systems that contain sensitive information; and

(4) to require mandatory periodic training for all persons involved in management, use, or operation of Federal computer systems that contain sensitive information.

SEC. 3. ESTABLISHMENT OF COMPUTER STANDARDS PROGRAM.

The Act of March 3, 1901 (15 U.S.C. 271-278h), is amended—

(1) in section 2(f), by striking out "and" at the end of paragraph (18), by striking out the period at the end of paragraph (19) and inserting in lieu thereof: "; and", and by inserting after such paragraph the following:

"(20) the study of computer systems (as that term is defined in section 20(d) of this Act) and their use to control machinery and processes.";

(2) by redesignating section 20 as section 22, and by inserting after section 19 the following new sections:

"Sec. 20. (a) The National Bureau of Standards shall—

"(1) have the mission of developing standards, guidelines, and associated methods and techniques for computer systems,

"(2) except as described in paragraph (3) of this subsection (relating to security standards), develop uniform standards and guidelines for Federal computer systems, except those systems excluded by section 2315 of title 10, United States Code, or section 3502(2) of title 44, United States Code;

"(3) have responsibility within the Federal Government for developing technical, management, physical, and administrative standards and guidelines for the cost-effective security and privacy of sensitive information in Federal computer systems except—

"(A) those systems excluded by section 2315 of title 10, United States Code, or section 3502(2) of title 44, United States Code; and

"(B) those systems which are protected at all times by procedures established for information which has been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept secret in the interest of national defense or foreign policy,

the primary purpose of which standards and guidelines shall be to control loss and unauthorized modification or disclosure of sensitive information in such systems and to prevent computer-related fraud and misuse;

"(4) submit standards and guidelines developed pursuant to paragraphs (2) and (3) of this subsection, along with recommendations as to the extent to which these should be made compulsory and binding, to the Secretary of Commerce for promulgation under section 111(d) of the Federal Property and Administrative Services Act of 1949;

"(5) develop guidelines for use by operators of Federal computer systems that contain sensitive information in training their employees in security awareness and accepted security practice, as required by section 5 of the Computer Security Act of 1987; and

"(6) develop validation procedures for, and evaluate the effectiveness of, standards and guidelines developed pursuant to paragraphs (1), (2), and (3) of this subsection through research and liaison with other government and private agencies.

"(b) In fulfilling subsection (a) of this section, the National Bureau of Standards is authorized—

"(1) to assist the private sector, upon request, in using and applying the results of the programs and activities under this section;

"(2) to make recommendations, as appropriate, to the Administrator of General Services on policies and regulations proposed pursuant to section 111(d) of the Federal Property and Administrative Services Act of 1949;

"(3) as requested, to provide to operators of Federal computer systems technical assistance in implementing the standards and guidelines promulgated pursuant to section 111(d) of the Federal Property and Administrative Services Act of 1949;

"(4) to assist, as appropriate, the Office of Personnel Management in developing regulations pertaining to training, as required by section 5 of the Computer Security Act of 1987;

"(5) to perform research and to conduct studies, as needed, to determine the nature and extent of the vulnerabilities of, and to

device techniques for the cost-effective security and privacy of sensitive information in Federal computer systems; and

"(6) to coordinate closely with other agencies and offices (including, but not limited to, the Departments of Defense and Energy, the National Security Agency, the General Accounting Office, the Office of Technology Assessment, and the Office of Management and Budget)—

"(A) to assure maximum use of all existing and planned programs, materials, studies, and reports relating to computer systems security and privacy, in order to avoid unnecessary and costly duplication of effort; and

"(B) to assure, to the maximum extent feasible, that standards developed pursuant to subsection (a) (3) and (5) are consistent and compatible with standards and procedures developed for the protection of information in Federal computer systems which is authorized under criteria established by Executive order or an Act of Congress to be kept secret in the interest of national defense or foreign policy.

"(c) For the purposes of—

"(1) developing standards and guidelines for the protection of sensitive information in Federal computer systems under subsections (a)(1) and (a)(3), and

"(2) performing research and conducting studies under subsection (b)(5),

the National Bureau of Standards shall draw upon computer system technical security guidelines developed by the National Security Agency to the extent that the National Bureau of Standards determines that such guidelines are consistent with the requirements for protecting sensitive information in Federal computer systems.

"(d) As used in this section—

"(1) the term 'computer system'—

"(A) means any equipment or interconnected system or subsystems of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception, of data or information; and

"(B) includes—

"(i) computers;

"(ii) ancillary equipment;

"(iii) software, firmware, and similar procedures;

"(iv) services, including support services; and

"(v) related resources as defined by regulations issued by the Administrator for General Services pursuant to section 111 of the Federal Property and Administrative Services Act of 1949;

"(2) the term 'Federal computer system'—

"(A) means a computer system operated by a Federal agency or by a contractor of a Federal agency or other organization that processes information (using a computer system) on behalf of the Federal Government to accomplish a Federal function; and

"(B) includes automatic data processing equipment as that term is defined in section 111(a)(2) of the Federal Property and Administrative Services Act of 1949;

"(3) the term 'operator of a Federal computer system' means a Federal agency, contractor of a Federal agency, or other organization that processes information using a computer

system on behalf of the Federal Government to accomplish a Federal function;

"(4) the term 'sensitive information' means any information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under section 552a of title 5, United States Code (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept secret in the interest of national defense or foreign policy; and

"(5) the term 'Federal agency' has the meaning given such term by section 3(b) of the Federal Property and Administrative Services Act of 1949.

"SEC. 21. (a) There is hereby established a Computer System Security and Privacy Advisory Board within the Department of Commerce. The Secretary of Commerce shall appoint the chairman of the Board. The Board shall be composed of twelve additional members appointed by the Secretary of Commerce as follows:

"(1) four members from outside the Federal Government who are eminent in the computer or telecommunications industry, at least one of whom is representative of small or medium sized companies in such industries;

"(2) four members from outside the Federal Government who are eminent in the fields of computer or telecommunications technology, or related disciplines, but who are not employed by or representative of a producer of computer or telecommunications equipment; and

"(3) four members from the Federal Government who have computer systems management experience, including experience in computer systems security and privacy, at least one of whom shall be from the National Security Agency.

"(b) The duties of the Board shall be—

"(1) to identify emerging managerial, technical, administrative, and physical safeguard issues relative to computer systems security and privacy;

"(2) to advise the Bureau of Standards and the Secretary of Commerce on security and privacy issues pertaining to Federal computer systems; and

"(3) to report its findings to the Secretary of Commerce, the Director of the Office of Management and Budget, the Director of the National Security Agency, and the appropriate committees of the Congress.

"(c) The term of office of each member of the Board shall be four years, except that—

"(1) of the initial members, three shall be appointed for terms of one year, three shall be appointed for terms of two years, three shall be appointed for terms of three years, and three shall be appointed for terms of four years; and

"(2) any member appointed to fill a vacancy in the Board shall serve for the remainder of the term for which his predecessor was appointed.

"(d) The Board shall not act in the absence of a quorum, which shall consist of seven members.

"(e) Members of the Board, other than full-time employees of the Federal Government, while attending meetings of such committees or while otherwise performing duties at the request of the Board

15 USC

Reports

Chairman while away from the home a major part of business, and be allowed travel expenses in accordance with subchapter I, chapter 57 of title 5, United States Code.

"(f) To provide the staff services necessary to assist the Board in carrying out its functions, the Board may utilize personnel from the National Bureau of Standards or any other agency of the Federal Government with the consent of the head of the agency.

"(g) As used in this section, the terms 'computer system' and 'Federal computer system' have the meanings given in section 20(d) of this Act.";

(3) by adding at the end thereof the following new section: "SEC. 23. This Act may be cited as the National Bureau of Standards Act."

SEC. 4. AMENDMENT TO BROOKS ACT.

Section 111(d) of the Federal Property and Administrative Services Act of 1949 (40 U.S.C. 759(d)) is amended to read as follows:

"(d)(1) The Secretary of Commerce shall, on the basis of standards and guidelines developed by the National Bureau of Standards pursuant to section 20(a) (2) and (3) of the National Bureau of Standards Act, promulgate standards and guidelines pertaining to Federal computer systems, making such standards compulsory and binding to the extent to which the Secretary determines necessary to improve the efficiency of operation or security and privacy of Federal computer systems. The President may disapprove or modify such standards and guidelines if he determines such action to be in the public interest. The President's authority to disapprove or modify such standards and guidelines may not be delegated. Notice of such disapproval or modification shall be submitted promptly to the Committee on Government Operations of the House of Representatives and the Committee on Governmental Affairs of the Senate and shall be published promptly in the Federal Register. Upon receiving notice of such disapproval or modification, the Secretary of Commerce shall immediately rescind or modify such standards or guidelines as directed by the President.

"(2) The head of a Federal agency may employ standards for the cost-effective security and privacy of sensitive information in a Federal computer system within or under the supervision of that agency that are more stringent than the standards promulgated by the Secretary of Commerce, if such standards contain, at a minimum, the provisions of those applicable standards made compulsory and binding by the Secretary of Commerce.

"(3) The standards determined to be compulsory and binding may be waived by the Secretary of Commerce in writing upon a determination that compliance would adversely affect the accomplishment of the mission of an operator of a Federal computer system, or cause a major adverse financial impact on the operator which is not offset by Government-wide savings. The Secretary may delegate to the head of one or more Federal agencies authority to waive such standards to the extent to which the Secretary determines such action to be necessary and desirable to allow for timely and effective implementation of Federal computer systems standards. The head of such agency may redelegate such authority only to a senior official designated pursuant to section 3506(b) of title 44, United States Code. Notice of each such waiver and delegation shall be transmitted promptly to the Committee on Government Operations of the House of Representatives and the Committee on Governmental

Affairs of the State shall be published from time to time in the Register.

"(4) The Administrator shall revise the Federal information resources management regulations (41 CFR ch. 201) to be consistent with the standards and guidelines promulgated by the Secretary of Commerce under this subsection.

"(5) As used in this subsection, the terms 'Federal computer system' and 'operator of a Federal computer system' have the meanings given in section 20(d) of the National Bureau of Standards Act."

SEC. 5. FEDERAL COMPUTER SYSTEM SECURITY TRAINING.

(a) IN GENERAL.—Each Federal agency shall provide for the mandatory periodic training in computer security awareness and accepted computer security practice of all employees who are involved with the management, use, or operation of each Federal computer system within or under the supervision of that agency. Such training shall be—

(1) provided in accordance with the guidelines developed pursuant to section 20(a)(5) of the National Bureau of Standards Act (as added by section 3 of this Act), and in accordance with the regulations issued under subsection (c) of this section for Federal civilian employees; or

(2) provided by an alternative training program approved by the head of that agency on the basis of a determination that the alternative training program is at least as effective in accomplishing the objectives of such guidelines and regulations.

(b) TRAINING OBJECTIVES.—Training under this section shall be started within 60 days after the issuance of the regulations described in subsection (c). Such training shall be designed—

(1) to enhance employees' awareness of the threats to and vulnerability of computer systems; and

(2) to encourage the use of improved computer security practices.

(c) REGULATIONS.—Within six months after the date of the enactment of this Act, the Director of the Office of Personnel Management shall issue regulations prescribing the procedures and scope of the training to be provided Federal civilian employees under subsection (a) and the manner in which such training is to be carried out.

SEC. 6. ADDITIONAL RESPONSIBILITIES FOR COMPUTER SYSTEMS SECURITY AND PRIVACY.

(a) IDENTIFICATION OF SYSTEMS THAT CONTAIN SENSITIVE INFORMATION.—Within 6 months after the date of enactment of this Act, each Federal agency shall identify each Federal computer system, and system under development, which is within or under the supervision of that agency and which contains sensitive information.

(b) SECURITY PLAN.—Within one year after the date of enactment of this Act, each such agency shall, consistent with the standards, guidelines, policies, and regulations prescribed pursuant to section 111(d) of the Federal Property and Administrative Services Act of 1949, establish a plan for the security and privacy of each Federal computer system identified by that agency pursuant to subsection (a) that is commensurate with the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of the information contained in such system. Copies of each such plan shall be transmitted to the National Bureau of Standards

Regulation

40 USC 71

40 USC 7

and the National Security Agency for advice and comment. A summary of such plan shall be included in the agency's five-year plan required by section 3505 of title 44, United States Code. Such plan shall be subject to disapproval by the Director of the Office of Management and Budget. Such plan shall be revised annually as necessary.

40 USC 759 note. **SEC. 7. DEFINITIONS.**

As used in this Act, the terms "computer system", "Federal computer system", "operator of a Federal computer system", "sensitive information", and "Federal agency" have the meanings given in section 20(d) of the National Bureau of Standards Act (as added by section 3 of this Act).

40 USC 759 note. **SEC. 8. RULES OF CONSTRUCTION OF ACT.**

Nothing in this Act, or in any amendment made by this Act, shall be construed—

(1) to constitute authority to withhold information sought pursuant to section 552 of title 5, United States Code; or

Public
information.

(2) to authorize any Federal agency to limit, restrict, regulate, or control the collection, maintenance, disclosure, use, transfer, or sale of any information (regardless of the medium in which the information may be maintained) that is—

(A) privately-owned information;

(B) disclosable under section 552 of title 5, United States Code, or other law requiring or authorizing the public disclosure of information; or

(C) public domain information.

Approved January 8, 1988.

LEGISLATIVE HISTORY—H.R. 145:

HOUSE REPORTS: No. 100-153, Pt. 1 (Comm. on Science, Space, and Technology) and Pt. 2 (Comm. on Government Operations).

CONGRESSIONAL RECORD, Vol. 133 (1987):

June 22, considered and passed House.

Dec. 21, considered and passed Senate.

PUBLIC LAW 100-236 [H.R. 1162]; January 8, 1988

SELECTION OF COURT FOR MULTIPLE APPEALS

For Legislative History of Act, see p. 3198.

An Act to amend title 28, United States Code, to provide for the selection of the court to decide multiple appeals filed with respect to the same agency order.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SELECTION OF COURT FOR MULTIPLE APPEALS.

Section 2112(a) of title 28, United States Code, is amended by striking out the last three sentences and inserting in lieu thereof the following: "If proceedings are instituted in two or more courts of appeals with respect to the same order, the following shall apply:

"(1) If within ten days after issuance of the order the agency, board, commission, or officer concerned receives, from the persons instituting the proceedings, the petition for review with respect to the same order, the agency, board, commission, or officer shall proceed in accordance with paragraph (3) of this subsection. If within ten days after the issuance of the order the agency, board, commission, or officer concerned receives, from the persons instituting the proceedings, the petition for review with respect to the same order, the agency, board, commission, or officer shall file the record in that court notwithstanding any institution in any other court of appeals of proceedings for review of that order. In all other cases in which proceedings have been instituted in two or more courts of appeals with respect to the same order, the agency, board, commission, or officer concerned shall file the record in the court in which the proceedings with respect to the order were first instituted.

"(2) For purposes of paragraph (1) of this subsection, a petition or other pleading which institutes proceedings in a court of appeals and which is stamped by the court with the date of filing shall constitute the petition for review. The agency, board, commission, or officer, as the case may be, shall designate by rule the office and the officer who must receive and file petitions for review under paragraph (1).

"(3) If an agency, board, commission, or officer receives more than one petition for review of an order in accordance with the first sentence of paragraph (1) of this subsection, the agency, board, commission, or officer shall, promptly after the expiration of the ten-day period specified in that sentence, so select the judicial panel on multidistrict litigation authorized by section 1407 of this title, in such form as that panel shall prescribe. The judicial panel on multidistrict litigation shall, by means of a random selection, designate one court of appeals, from among the courts of appeals in which petitions for review have been filed and received within the ten-day period specified in the first sentence of paragraph (1), in which the record is to be filed. The designated court shall issue an order consolidating the petitions for review in that court of appeals. The judicial panel on multidistrict

offered by a foreign government, and to the acceptance and retention by an employee of the Institute of any form of financial or other assistance provided by a foreign government as compensation for or as a means of defraying expenses associated with the performance of scientific or engineering activities or the exchange of scientific or technical information, in any case where the acceptance of such fellowship, lectureship, or position or the acceptance and retention of such assistance is determined by the Secretary to be appropriate and consistent with the interests of the United States. For the purposes of this subsection, the definitions appearing in section 7342(a) of Title 5 apply. Civil actions may be brought and penalties assessed against any employee who knowingly accepts and retains assistance from a foreign government not consented to by this subsection in the same manner as is prescribed by section 7342(h) of Title 5.

(c) Prohibition on use of appropriations inapplicable

Provisions of law prohibiting the use of any part of any appropriation for the payment of compensation to any employee or officer of the Government of the United States who is not a citizen of the United States shall not apply to the payment of compensation to scientific or engineering personnel of the Institute.

(Mar. 3, 1901, c. 872, § 17, as added Oct. 15, 1980, Pub.L. 96-461, § 9, 94 Stat. 2051, and amended Aug. 23, 1988, Pub.L. 100-418, Title V, § 5115(a)(1), 102 Stat. 1433.)

Codification. Section 9 of Pub.L. 96-461, in addition to enacting this section, enacted a provision set out as a note under this section.

Prior Provisions. A prior section 278g, Act Mar. 3, 1901, c. 872, § 17, as added Mar. 1, 1968, Pub.L. 90-259, Title I, § 102, 82 Stat. 35, which related to grants to states, local governments, other nonfederal public agencies, and non-profit institutions, reimbursement of federal agencies, delegation of powers, advance of public moneys, cooperation of federal agencies, and issuance of rules and regulations, was repealed by Pub.L. 93-498, § 18, Oct. 29, 1974, 88 Stat. 1545.

1988 Amendment. Pub.L. 100-418, § 5115(a)(1), substituted "Institute" for "National Bureau of Standards" wherever appearing.

Effective Date of 1980 Amendment. Section 11 of Pub.L. 96-461 provided that: "The effective date of sections 8 and 9 of this Act [enacting this section, amending section 278d of this title, and

enacting a provision set out as a note under this section] shall be October 1, 1980."

Congressional Declaration of Purpose. Section 9 of Pub.L. 96-461; as amended Pub.L. 100-418, Title V, § 5115(c), Aug. 23, 1988, 102 Stat. 1433, provided in part that:

"In order to develop and strengthen the expertise of the National Institute of Standards and Technology in science and engineering, to enhance the Secretary's ability to maintain the Institute's programs at the forefront of worldwide developments in science and engineering, and to cooperate in international scientific activities, the Act of March 3, 1901 (15 U.S.C. 271-278h), as amended [sections 271 to 278h of this title], is further amended by inserting immediately after section 16 the following new section [this section]."

Legislative History. For legislative history and purpose of Pub.L. 100-418, see 1988 U.S. Code Cong. and Adm. News, p. 1547.

§ 278g-1. Research fellowships and other financial assistance to students at institutions of higher education

The Director is authorized to expend up to 1 per centum of the funds appropriated for activities of the Institute in any fiscal year, as the Director may deem desirable, for awards of research fellowships and other forms of financial assistance to students at institutions of higher learning within the United States who show promise as present or future contributors to the mission of the Institute. The selection of persons to receive such fellowships and assistance shall be made on the basis of ability and of the relevance of the proposed work to the mission and programs of the Institute.

(Mar. 3, 1901, c. 872, § 18, as added Oct. 28, 1986, Pub.L. 99-574, § 6(a), 100 Stat. 3237, and amended Aug. 23, 1988, Pub.L. 100-418, Title V, § 5115(a)(1), 102 Stat. 1433.)

1988 Amendment. Pub.L. 100-418, § 5115(a)(1), substituted "Institute" for "National Bureau of Standards" the first place appearing, and for "Bureau" wherever subsequently appearing, respectively.

Effective Date. Section 6(b) of Pub.L. 99-574

section (a) [enacting this section] shall be effective October 1, 1986."

Legislative History. For legislative history and purpose of Pub.L. 99-574, see 1986 U.S. Code Cong. and Adm. News, p. 5435. See, also, Pub.L. 100-418, 1988 U.S. Code Cong. and Adm. News,

§ 278g-2. Post-doctoral fellowship program

The Institute, in conjunction with the National Academy of Sciences, shall establish and conduct a post-doctoral fellowship program which shall be organized and carried out in substantially the same manner as the National Academy of Sciences/National Research Council Post-Doctoral Research Associate Program that was in effect prior to 1986, and which shall include not less than twenty nor more than forty new fellows per fiscal year.

(Mar. 3, 1901, c. 872, § 19, as added Oct. 28, 1986, Pub.L. 99-574, § 8(a), 100 Stat. 3238, and amended Aug. 23, 1988, Pub.L. 100-418, Title V, § 5115(a)(1), 102 Stat. 1433.)

1988 Amendment. Pub.L. 100-418, § 5115(a)(1), substituted "Institute" for "National Bureau of Standards".

Effective Date. Section 8(b) of Pub.L. 99-574 provided that: "The amendments made by subsection (a) [enacting this section] shall be effective October 1, 1987."

Legislative History. For legislative history and purpose of Pub.L. 99-574, see 1986 U.S. Code Cong. and Adm. News, p. 5435. See, also, Pub.L. 100-418, 1988 U.S. Code Cong. and Adm. News, p. 1547.

§ 278g-3. Computer standards program

(a) Development of standards, guidelines, methods and techniques for computer systems

The Institute shall—

(1) have the mission of developing standards, guidelines, and associated methods and techniques for computer systems;

(2) except as described in paragraph (3) of this subsection (relating to security standards), develop uniform standards and guidelines for Federal computer systems, except those systems excluded by section 2315 of Title 10, or section 3502(2) of Title 44;

(3) have responsibility within the Federal Government for developing technical, management, physical, and administrative standards and guidelines for the cost-effective security and privacy of sensitive information in Federal computer systems except—

(A) those systems excluded by section 2315 of Title 10, or section 3502(2) of Title 44; and

(B) those systems which are protected at all times by procedures established for information which has been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept secret in the interest of national defense or foreign policy,

the primary purpose of which standards and guidelines shall be to control loss and unauthorized modification or disclosure of sensitive information in such systems and to prevent computer-related fraud and misuse;

(4) submit standards and guidelines developed pursuant to paragraphs (2) and (3) of this subsection, along with recommendations as to the extent to which these should be made compulsory and binding, to the Secretary of Commerce for promulgation under section 759(d) of Title 40;

(5) develop guidelines for use by operators of Federal computer systems that contain sensitive information in training their employees in security awareness and accepted security practice, as required by section 5 of the Computer Security Act of 1987; and

(6) develop validation procedures for, and evaluate the effectiveness of, standards and guidelines developed pursuant to paragraphs (1), (2), and (3) of this subsection through research and liaison with other government and private agencies.

(b) Technical assistance and implementation of standards developed

In fulfilling subsection (a) of this section, the Institute is authorized—

(1) to assist the private sector, upon request, in using and applying the results of the programs and activities under this section;

(2) to make recommendations, as appropriate, to the Administrator of General Services on policies and regulations proposed pursuant to section 759(d) of Title

(2) requested, to provide to operators of Federal computer systems technical assistance in implementing the standards and guidelines promulgated pursuant to section 759(d) of Title 40;

(4) to assist, as appropriate, the Office of Personnel Management in developing regulations pertaining to training, as required by section 5 of the Computer Security Act of 1987;

(5) to perform research and to conduct studies, as needed, to determine the nature and extent of the vulnerabilities of, and to devise techniques for the cost-effective security and privacy of sensitive information in Federal computer systems; and

(6) to coordinate closely with other agencies and offices (including, but not limited to, the Departments of Defense and Energy, the National Security Agency, the General Accounting Office, the Office of Technology Assessment, and the Office of Management and Budget)—

(A) to assure maximum use of all existing and planned programs, materials, studies, and reports relating to computer systems security and privacy, in order to avoid unnecessary and costly duplication of effort; and

(B) to assure, to the maximum extent feasible, that standards developed pursuant to subsection (a)(3) and (5) are consistent and compatible with standards and procedures developed for the protection of information in Federal computer systems which is authorized under criteria established by Executive order or an Act of Congress to be kept secret in the interest of national defense or foreign policy.

(c) Protection of sensitive information

For the purposes of—

(1) developing standards and guidelines for the protection of sensitive information in Federal computer systems under subsections (a)(1) and (a)(3), and

(2) performing research and conducting studies under subsection (b)(5),

the Institute shall draw upon computer system technical security guidelines developed by the National Security Agency to the extent that the Institute determines that such guidelines are consistent with the requirements for protecting sensitive information in Federal computer systems.

(d) Definitions

As used in this section—

(1) the term "computer system"—

(A) means any equipment or interconnected system or subsystems of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception, of data or information; and

(B) includes—

(i) computers;

(ii) ancillary equipment;

(iii) software, firmware, and similar procedures;

(iv) services, including support services; and

(v) related resources as defined by regulations issued by the Administrator for General Services pursuant to section 759 of Title 40;

(2) the term "Federal computer system"—

(A) means a computer system operated by a Federal agency or by a contractor of a Federal agency or other organization that processes information (using a computer system) on behalf of the Federal Government to accomplish a Federal function; and

(B) includes automatic data processing equipment as that term is defined in section 759(a)(2) of Title 40;

(3) the term "operator of a Federal computer system" means a Federal agency, contractor of a Federal agency, or other organization that processes information using a computer system on behalf of the Federal Government to accomplish a Federal function;

(4) the term "sensitive information" means any information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under section 552a of Title 5 (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept secret in the interest of national defense or foreign policy; and

(5) the term "Federal agency" has the meaning given such term by section 472(b) of Title 40.

(Mar. 3, 1901, c. 872, § 20, as added Jan. 8, 1988, Pub.L. 100-235, § 3(2), 101 Stat. 1724, and amended Aug. 23, 1988, Pub.L. 100-418, Title V, § 5115(a)(1), 102 Stat. 1483.)

References in Text. Section 5 of the Computer Security Act of 1987, referred to in subsections (a)(5) and (b)(4), is section 5 of Pub.L. 100-235, Jan. 8, 1988, 101 Stat. 1729, which is set out as a note under section 759 of Title 40, Public Buildings, Property, and Works.

1988 Amendment. Subsec. (a). Pub.L. 100-418, § 5115(a)(1), substituted "Institute" for "National Bureau of Standards" in provisions preceding par. (1).

Subsec. (b). Pub.L. 100-418, § 5115(a)(1), substituted "Institute" for "National Bureau of Standards" in provisions preceding par. (1).

Subsec. (c). Pub.L. 100-418, § 5115(a)(1), substituted "Institute" for "National Bureau of Standards" wherever appearing in provisions following numbered paragraphs.

Legislative History. For legislative history and purpose of Pub.L. 100-418, see 1988 U.S. Code Cong. and Adm. News, p. 1547.

§ 278g-4. Computer System Security and Privacy Advisory Board

(a) Establishment and composition

There is hereby established a Computer System Security and Privacy Advisory Board within the Department of Commerce. The Secretary of Commerce shall appoint the chairman of the Board. The Board shall be composed of twelve additional members appointed by the Secretary of Commerce as follows:

(1) four members from outside the Federal Government who are eminent in the computer or telecommunications industry, at least one of whom is representative of small or medium sized companies in such industries;

(2) four members from outside the Federal Government who are eminent in the fields of computer or telecommunications technology, or related disciplines, but who are not employed by or representative of a producer of computer or telecommunications equipment; and

(3) four members from the Federal Government who have computer systems management experience, including experience in computer systems security and privacy, at least one of whom shall be from the National Security Agency.

(b) Duties

The duties of the Board shall be—

(1) to identify emerging managerial, technical, administrative, and physical safeguard issues relative to computer systems security and privacy;

(2) to advise the Institute and the Secretary of Commerce on security and privacy issues pertaining to Federal computer systems; and

(3) to report its findings to the Secretary of Commerce, the Director of the Office of Management and Budget, the Director of the National Security Agency, and the appropriate committees of the Congress.

(c) Term of office

The term of office of each member of the Board shall be four years, except that—

(1) of the initial members, three shall be appointed for terms of one year, three shall be appointed for terms of two years, three shall be appointed for terms of three years, and three shall be appointed for terms of four years; and

(2) any member appointed to fill a vacancy in the Board shall serve for the remainder of the term for which his predecessor was appointed.

(d) Quorum

The Board shall not act in the absence of a quorum which shall consist of seven members.

(e) Allowance for travel expenses

Members of the Board, other than full-time employees of the Federal Government, while attending meetings of such committees or while otherwise performing duties at the request of the Board Chairman while away from their homes or a regular place of business, may be allowed travel expenses in accordance with subchapter I of chapter 57 of Title 5 [5 U.S.C.A. § 5701 et seq.].

(f) Staff services and utilization of federal personnel

To provide the staff services necessary to assist the Board in carrying out its functions, the Board may utilize personnel from the Institute or any other agency of the Federal Government with the consent of the head of the agency.

(g) Definitions

As used in this section, the terms "computer system" and "Federal computer system" have the meanings given in section 20(d) of this Act.

(Mar. 3, 1901, c. 872, § 21, as added Jan. 8, 1988, Pub.L. 100-235, § 3(2), 101 Stat. 1727, and amended Aug. 23, 1988, Pub.L. 100-418, Title V, § 5115(a)(1), 102 Stat. 1433.)

1988 Amendment. Subsec. (b)(2). Pub.L. 100-418, § 5115(a)(1), which directed that "Institute" be substituted for "National Bureau of Standards", "Bureau" and "bureau", wherever appearing, was executed to subsec. (b)(2) by substituting "Institute" for "Bureau of Standards" as the probable intent of Congress in view of the change of name of the National Bureau of Standards to the National Institute of Standards and Technology

by section 271(b)(1) of this title, as amended by Pub.L. 100-418.

Subsec. (f). Pub.L. 100-418, § 5115(a)(1), substituted "Institute" for "National Bureau of Standards".

Legislative History. For legislative history and purpose of Pub.L. 100-418, see 1988 U.S. Code Cong. and Adm. News, p. 1547.

§ 278h. Appropriations; availability

Appropriations to carry out the provisions of this chapter may remain available for obligation and expenditure for such period or periods as may be specified in the Acts making such appropriations.

(Mar. 3, 1901, c. 872, § 22, formerly § 18, as added June 22, 1972, Pub.L. 92-317, § 3(a), 86 Stat. 235, and amended July 21, 1978, Pub.L. 95-322, § 2(b), 92 Stat. 395; Oct. 15, 1980, Pub.L. 96-461, § 10, 94 Stat. 2052; renumbered § 19, Oct. 28, 1986, Pub.L. 99-574, § 6(a), 100 Stat. 3237; renumbered § 20, Oct. 28, 1986, Pub.L. 99-574, § 8(a), 100 Stat. 3238; renumbered § 22, Jan. 8, 1988, Pub.L. 100-235, § 3(2), 101 Stat. 1724.)

References in Text. This chapter, referred to in text, in the original read "this Act" meaning Act Mar. 3, 1901, c. 872, which comprises all sections of this chapter other than sections 279 to 282.

1980 Amendment. Pub.L. 96-461 substituted "Appropriations" for "(a) Appropriations" and struck out subsec. (b), which authorized appropriations to carry out provisions of this chapter, including the Working Capital Fund referred to in section 278b(a) of this title, but excluding section

278f of this title, of such sums as may be necessary for each of the fiscal years 1979 and 1980.

1978 Amendment. Subsec. (a). Pub.L. 95-322, § 2(b)(1), designated existing provisions as subsec. (a).

Subsec. (b). Pub.L. 95-322, § 2(b)(2), added subsec. (b).

Legislative History. For legislative history and purpose of Pub.L. 99-574, see 1986 U.S. Code Cong. and Adm. News, p. 5435.

§ 278i. Reports to Congress

(a) The Director shall keep the Committee on Commerce, Science, and Transportation of the Senate and the Committee on Science, Space, and Technology of the House of Representatives fully and currently informed with regard to all of the activities of the Institute.

(b) The Director shall justify in writing all changes in policies regarding fees for standard reference materials and calibration services occurring after June 30, 1987, including a description of the anticipated impact of any proposed changes on demand for and anticipated revenues from the materials and services. Changes in policy and fees shall not be effective unless and until the Director has submitted the proposed schedule and justification to the Congress and 30 days on which both Houses of Congress are in session have elapsed since such submission, except that the requirement of this sentence shall not apply with respect to adjustments which are

based solely on changes in the costs of raw materials or of producing and delivering standard reference materials or calibration services.

(Mar. 3, 1901, c. 872, § 23, as added Aug. 23, 1988, Pub.L. 100-418, Title V, § 5114(2), 102 Stat. 1432.)

Legislative History. For legislative history and purpose of Pub.L. 100-418, see 1988 U.S. Code Cong. and Adm. News, p. 1547.

§ 278j. Studies by the National Research Council

The Director may periodically contract with the National Research Council for advice and studies to assist the Institute to serve United States industry and science. The subjects of such advice and studies may include—

(1) the competitive position of the United States in key areas of manufacturing and emerging technologies and research activities which would enhance that competitiveness;

(2) potential activities of the Institute, in cooperation with industry and the States, to assist in the transfer and dissemination of new technologies for manufacturing and quality assurance; and

(3) identification and assessment of likely barriers to widespread use of advanced manufacturing technology by the United States workforce, including training and other initiatives which could lead to a higher percentage of manufacturing jobs of United States companies being located within the borders of our country.

(Mar. 3, 1901, c. 872, § 24, as added Aug. 23, 1988, Pub.L. 100-418, Title V, § 5114(2), 102 Stat. 1432.)

Legislative History. For legislative history and purpose of Pub.L. 100-418, see 1988 U.S. Code Cong. and Adm. News, p. 1547.

§ 278k. Regional centers for the transfer of manufacturing technology

(a) Creation and support of Centers; affiliations; merit review in determining awards; objectives

The Secretary, through the Director and, if appropriate, through other officials, shall provide assistance for the creation and support of Regional Centers for the Transfer of Manufacturing Technology (hereafter in this chapter referred to as the "Centers"). Such centers shall be affiliated with any United States-based nonprofit institution or organization, or group thereof, that applies for and is awarded financial assistance under this section in accordance with the description published by the Secretary in the Federal Register under subsection (c)(2) of this section. Individual awards shall be decided on the basis of merit review. The objective of the Centers is to enhance productivity and technological performance in United States manufacturing through—

(1) the transfer of manufacturing technology and techniques developed at the Institute to Centers and, through them, to manufacturing companies throughout the United States;

(2) the participation of individuals from industry, universities, State governments, other Federal agencies, and, when appropriate, the Institute in cooperative technology transfer activities;

(3) efforts to make new manufacturing technology and processes usable by United States-based small- and medium-sized companies;

(4) the active dissemination of scientific, engineering, technical, and management information about manufacturing to industrial firms, including small- and medium-sized manufacturing companies; and

(5) the utilization, when appropriate, of the expertise and capability that exists in Federal laboratories other than the Institute.

(b) Activities of Centers

The activities of the Centers shall include

(b) Function and availability of Fund

The Fund shall—

(1) assume all of the liabilities, obligations, and commitments of the funds described in subparagraphs (A) and (B) of subsection (a)(1); and

(2) be available for expenses, including personal services and other costs, and for procurement (by lease, purchase, transfer, or otherwise) for efficiently providing information technology resources to Federal agencies and for the efficient management, coordination, operation, and utilization of such resources.

(c) Contract authority

(1) In the operation of the Fund, the Administrator is authorized to enter into multiyear contracts for the provision of information technology hardware, software, or services for periods not in excess of five years, if—

(A) funds are available and adequate for payment of the costs of such contract for the first fiscal year and any costs of cancellation or termination;

(B) such contract is awarded on a fully competitive basis; and

(C) the Administrator determines that—

(i) the need for the information technology hardware, software, or services being provided will continue over the period of the contract;

(ii) the use of the multiyear contract will yield substantial cost savings when compared with other methods of providing the necessary resources; and

(iii) such a method of contracting will not exclude small business participation.

(2) Any cancellation costs incurred with respect to a contract entered into under this subsection shall be paid from currently available funds in the Fund.

(3) This subsection shall not be construed to limit the authority of the Administrator to procure equipment and services under section 481 of this title.

(d) Transfer of uncommitted balances

Following the close of each fiscal year, the uncommitted balance of any funds remaining in the Fund, after making provision for anticipated operating needs as determined by the Office of Management and Budget, shall be transferred to the general fund of the Treasury as miscellaneous receipts.

(e) Annual report

A report on the operation of the Fund shall be made annually by the Administrator to the Director of the Office of Management and Budget. Such report shall identify any proposed increases to the capital of the Fund and shall include a report on information processing equipment inventory, utilization, and acquisition.

(f) Information technology resources

For purposes of this section, the term "information technology resources" includes any service or equipment which had been acquired or provided under this section or section 759 of this title, including other information processing and transmission equipment, software, systems, operating facilities, supplies, and services related thereto, and maintenance and repair thereof.

(As amended Oct. 18, 1986, Pub.L. 99-500, Title I, § 101(m), [Title VIII, § 821], 100 Stat. 1783-345; Oct. 80, 1986, Pub.L. 99-591, Title I, § 101(m), [Title VIII, § 821], 100 Stat. 3341-345.)

1986 Amendments. Pub.L. 99-500 substituted provision relating to the Information Technology Fund for provision relating to the Federal telecommunications fund.

Pub.L. 99-591 made an amendment identical to Pub.L. 99-500.

Effective Date of 1986 Amendment. Section 833 of Title VIII of the Treasury, Postal Service, and General Government Appropriations Act, 1987 [Pub.L. 99-500, Title I, § 101(m), Oct. 18,

§ 101(m), Oct. 30, 1986, 100 Stat. 3341-345], provided that: "This title and the amendments made by this title [amending this section, sections 751 and 759 of this title, and sections 3501, 3502, 3503, 3503 note, 3504 to 3507, 3511, 3514, and 3520 of Title 44, Public Printing and Documents, repealing section 759 note of this title, and enacting provisions set out as a note under section 3503 of Title 44] shall take effect on the date of enactment of the Act [Oct. 18, 1986]."

of section 821 and the amendments made by such section [amending this section and section 759 of this title and section 3504 of Title 44] shall take effect on January 1, 1987."

Delegation of Functions. All functions, authority, and responsibility of the Director of the Office of Management and Budget under this section were delegated to the Administrator for the Office

of Information and Regulatory Affairs in the Office of Management and Budget pursuant to Pub. L. 96-511, § 3(b), Dec. 11, 1980, 94 Stat. 2825, set out as a note under section 3503 of Title 44, Public Printing and Documents.

Legislative History. For legislative history and purpose of Pub.L. 99-591, see 1986 U.S. Code Cong. and Adm. News, p. 5627.

§ 759. Procurement, maintenance, operation and utilization of automatic data processing equipment

(a) Authority of Administrator to coordinate and provide for purchase, lease and maintenance of equipment by Federal agencies

(1) The Administrator is authorized and directed to coordinate and provide for the economic and efficient purchase, lease, and maintenance of automatic data processing equipment by Federal agencies.

(2)(A) For purposes of this section, the term "automatic data processing equipment" means any equipment or interconnected system or subsystems of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching interchange, transmission, or reception, of data or information—

(i) by a Federal agency, or

(ii) under a contract with a Federal agency which—

(I) requires the use of such equipment, or

(II) requires the performance of a service or the furnishing of a product which is performed or produced making significant use of such equipment.

(B) Such term includes—

(i) computers;

(ii) ancillary equipment;

(iii) software, firmware, and similar procedures;

(iv) services, including support services; and

(v) related resources as defined by regulations issued by the Administrator for General Services.

(3) This section does not apply to—

(A) automatic data processing equipment acquired by a Federal contractor which is incidental to the performance of a Federal contract;

(B) radar, sonar, radio, or television equipment;

(C) the procurement by the Department of Defense of automatic data processing equipment or services if the function, operation, or use of which—

(i) involves intelligence activities;

(ii) involves cryptologic activities related to national security;

(iii) involves the command and control of military forces;

(iv) involves equipment which is an integral part of a weapon or weapons system; or

(v) is critical to the direct fulfillment of military or intelligence missions, provided that this exclusion shall not include automatic data processing equipment used for routine administrative and business applications such as payroll, finance, logistics, and personnel management; or

(D) the procurement of automatic data processing equipment or services by the Central Intelligence Agency.

(b) Procurement, maintenance and repair of equipment; transfer between agencies; joint utilization; establishment and operation of equipment pools and data processing centers; delegation of Administrator's authority

[See main volume for text of (1) and (2)]

(3) If the Administrator finds that a senior official of an agency designated pursuant to section 3506 of Title 44 is suitably indoctrinated by the

and effectively procurements under this section, the Administrator may delegate to such official the authority to lease, purchase, or maintain automatic data processing equipment pursuant to paragraph (2) of this subsection, except that any such delegation shall not relieve the Administrator of the responsibilities assigned to the Administrator under this section. A delegation by the Administrator under this subsection shall not preclude the Administrator from reviewing individual procurement requests if the Administrator determines that circumstances warrant such a review. The Administrator shall retain authority to revoke such delegations, both in general and with regard to any specific matter. In acting for the Administrator, any official to whom approval authority has been delegated under this subsection shall comply fully with the rules and regulations promulgated by the Administrator.

(c) Inapplicability of inconsistent provisions of law

The proviso following paragraph (4) in section 481(a) of this title and the provisions of section 474 of this title shall have no application in the administration of this section. No other provision of this Act or any other Act which is inconsistent with the provisions of this section shall be applicable in the administration of this section.

(d) Standards and guidelines for Federal computer systems; promulgation, disapproval or modification, etc.

(1) The Secretary of Commerce shall, on the basis of standards and guidelines developed by the National Bureau of Standards pursuant to section 278g-3(a)(2) and (3) of Title 15 promulgate standards and guidelines pertaining to Federal computer systems, making such standards compulsory and binding to the extent to which the Secretary determines necessary to improve the efficiency of operation or security and privacy of Federal computer systems. The President may disapprove or modify such standards and guidelines if he determines such action to be in the public interest. The President's authority to disapprove or modify such standards and guidelines may not be delegated. Notice of such disapproval or modification shall be submitted promptly to the Committee on Government Operations of the House of Representatives and the Committee on Governmental Affairs of the Senate and shall be published promptly in the Federal Register. Upon receiving notice of such disapproval or modification, the Secretary of Commerce shall immediately rescind or modify such standards or guidelines as directed by the President.

(2) The head of a Federal agency may employ standards for the cost-effective security and privacy of sensitive information in a Federal computer system within or under the supervision of that agency that are more stringent than the standards promulgated by the Secretary of Commerce, if such standards contain, at a minimum, the provisions of those applicable standards made compulsory and binding by the Secretary of Commerce.

(3) The standards determined to be compulsory and binding may be waived by the Secretary of Commerce in writing upon a determination that compliance would adversely affect the accomplishment of the mission of an operator of a Federal computer system, or cause a major adverse financial impact on the operator which is not offset by Government-wide savings. The Secretary may delegate to the head of one or more Federal agencies authority to waive such standards to the extent to which the Secretary determines such action to be necessary and desirable to allow for timely and effective implementation of Federal computer systems standards. The head of such agency may redelegate such authority only to a senior official designated pursuant to section 3506(b) of Title 44. Notice of each such waiver and delegation shall be transmitted promptly to the Committee on Government Operations of the House of Representatives and the Committee on Governmental Affairs of the Senate and shall be published promptly in the Federal Register.

(4) The Administrator shall revise the Federal information resources management regulations (41 CFR ch. 201) to be consistent with the standards and guidelines promulgated by the Secretary of Commerce under this subsection.

(5) As used in this subsection, the terms "Federal computer system" and "operator of a Federal computer system" have the meanings given in section 278g-3(d) of

(e) Limitations on authority of Administrator and Secretary of Commerce; notice and review of Administrator's determinations

The authority conferred upon the Administrator and the Secretary of Commerce by this section shall be exercised subject to direction by the President and to fiscal and policy control exercised by the Office of Management and Budget. Authority so conferred upon the Administrator shall not be so construed as to impair or interfere with the determination by agencies of their individual automatic data processing equipment requirements, including the development of specifications for and the selection of the types and configurations of equipment needed. The Administrator shall not interfere with, or attempt to control in any way, the use made of automatic data processing equipment or components thereof by any agency. The Administrator shall provide adequate notice to all agencies and other users concerned with respect to each proposed determination whether or not the automatic data processing equipment will be provided by the Administrator or whether or not the authority to lease, purchase, or maintain the equipment will be delegated. If the Administrator denies an agency procurement request such denial shall be subject to review and decision by the Director of the Office of Management and Budget, unless the President otherwise directs. Such review and decision shall be made only on the basis of a written appeal, and such written appeal, together with any written communications to the Administrator or any officer or employee of the Office of Management and Budget concerning such denial shall be made available to the public.

(f) Automated data processing dispute resolution

(1) Upon request of an interested party in connection with any procurement conducted which is subject to this section (including procurements subject to delegation of procurement authority), the board of contract appeals of the General Services Administration (hereafter in this subsection referred to as the "board"), shall review any decision by a contracting officer alleged to violate a statute or regulation. Such review shall be conducted under the standard applicable to review of contracting officer final decisions by boards of contract appeals. The authority of the board to conduct such review shall include the authority to determine whether any procurement is subject to this section and the authority to review regulations to determine their consistency with applicable statutes.

A proceeding, decision, or order of the board pursuant to this subsection shall not be subject to interlocutory appeal or review. An interested party who has filed a protest under subchapter V of chapter 35 of Title 31, with respect to a procurement or proposed procurement may not file a protest with respect to that procurement or proposed procurement under this subsection.

(2)(A) When a protest under this subsection is filed before the award of a contract in a protested procurement, the board, at the request of an interested party and within 10 days of the filing of the protest, shall hold a hearing to determine whether the board should suspend the procurement authority of the Administrator or the Administrator's delegation of procurement authority for the protested procurement on an interim basis until the board can decide the protest.

(B) The board shall suspend the procurement authority of the Administrator or the Administrator's delegation of procurement authority unless the Federal agency concerned establishes that—

(i) absent action by the board, contract award is likely to occur within 30 days of the hearing; and

(ii) urgent and compelling circumstances which significantly affect interests of the United States will not permit waiting for the decision of the board.

(3)(A) If the board receives notice of a protest under this subsection after the contract has been awarded but within 10 days after the contract award, the board shall, at the request of an interested party and within 10 days after the date of the filing of the protest, hold a hearing to determine whether the board should suspend the procurement authority of the Administrator or the Administrator's delegation of procurement authority for the challenged procurement on an interim basis until the board can decide the protest.

(B) The board shall suspend the procurement authority of the Administrator or

r the contract which are not previously delivered and accepted unless the Federal agency concerned establishes that urgent and compelling circumstances which significantly affect interests of the United States will not permit waiting for the decision of the board.

(4)(A) The board shall conduct such proceedings and allow such discovery as may be required for the expeditious, fair, and reasonable resolution of the protest.

(B) Subject to any deadlines imposed by section 9(a) of the Contract Disputes Act of 1978 (41 U.S.C. 608(a)) [41 U.S.C.A. § 608(a)], the board shall give priority to protests filed under this subsection. The board shall issue its final decision within 45 working days after the date of the filing of the protest, unless the board's chairman determines that the specific and unique circumstances of the protest require a longer period, in which case the board shall issue such decision within the longer period determined by the chairman.

(C) The board may dismiss a protest the board determines is frivolous or which, on its face, does not state a valid basis for protest.

(5)(A) In making a decision on the merits of protests brought under this section, the board shall accord due weight to the policies of this section and the goals of economic and efficient procurement set forth in this section. The board may consider any decision, determination, opinion, or statement made by the Director of the Office of Management and Budget or any officer of any other Federal agency regarding applicability of this section to a particular procurement, and may request the advice of the Director or such officer with regard to such applicability, but shall not be bound by any such decision, determination, opinion, or statement when determining whether a procurement is subject to this section.

(B) If the board determines that a challenged agency action violates a statute or regulation or the conditions of any delegation of procurement authority issued pursuant to this section, the board may suspend, revoke, or revise the procurement authority of the Administrator or the Administrator's delegation of procurement authority applicable to the challenged procurement.

(C) Whenever the board makes such a determination, it may, in accordance with section 1304 of Title 31, further declare an appropriate interested party to be entitled to the costs of—

- (i) filing and pursuing the protest, including reasonable attorney's fees, and
- (ii) bid and proposal preparation.

(6)(A) The final decision of the board may be appealed by the head of the Federal agency concerned and by any interested party, including interested parties who intervene in any protest filed under this subsection, as set forth in the Contract Disputes Act of 1978 (41 U.S.C. 601 et seq.) [41 U.S.C.A. § 601 et seq.].

(B) If the board revokes, suspends, or revises the procurement authority of the Administrator or the Administrator's delegation of procurement authority after the contract award, the affected contract shall be presumed valid as to all goods or services delivered and accepted under the contract before the suspension, revocation, or revision of such procurement authority or delegation.

(C) Nothing contained in this subsection shall affect the board's power to order any additional relief which it is authorized to provide under any statute or regulation. However, the procedures set forth in this subsection shall only apply to procurements conducted under the authority contained in this section. In addition, nothing contained in this subsection shall affect the right of any interested party to file a protest with the contracting agency or to file an action in a district court of the United States or the United States Claims Court.

(8)¹ Not later than January 15, 1985, the board shall adopt and issue such rules and procedures as may be necessary to the expeditious disposition of protests filed under the authority of this subsection.

(9) For purposes of this subsection—

(A) the term "protest" means a written objection by an interested party to a solicitation by a Federal agency for bids or proposals for a proposed contract for the procurement of property or services or a written objection to a proposed award or the award of such a contract, and

(B) the term "interested party" means, with respect to a contract or proposed contract described in subparagraph (A), an actual or prospective bidder or offeror whose direct economic interest would be affected by the award of the contract or by failure to award the contract.

(g) Procurement from sole source or by specific make and model

The justifications and approvals required by section 253(f)(1) of Title 41 shall apply in the case of any procurement under this section for which the minimum needs are so restrictive that only one manufacturer is capable of satisfying such needs. Such procurement includes either a sole source procurement or a procurement by specific make and model. Such justification and approval shall be required notwithstanding that more than one bid or offer is made or that the procurement obtains price competition and such procurement shall be treated as a procurement using procedures other than competitive procedures for purposes of section 417(b) of Title 41.

(h) Redesignated (f)

(i) Redesignated (g)

(As amended Oct. 18, 1986, Pub.L. 99-500, Title I, § 101(m) [Title VIII, §§ 821(b)(1), 822-825], 100 Stat. 1783-342-1783-344; Oct. 30, 1986, Pub.L. 99-591, Title I, § 101(m) [Title VIII, §§ 821(b)(1), 822-825], 100 Stat. 3341-342-3341-344; Jan. 8, 1988, Pub.L. 100-235, § 4, 101 Stat. 1728.)

1 Subsec. (f) enacted without a par. (7).

References in Text. This Act, referred to in subsec. (c), is Act June 30, 1949, c. 288, 63 Stat. 377, as amended, known as the Federal Property and Administrative Services Act of 1949. For complete classification of this Act to the Code, see Short Title note set out under section 471 of this title and Tables volume.

The Contract Disputes Act of 1978, referred to in subsec. (f)(6)(A), is Pub.L. 95-563, Nov. 1, 1978, 92 Stat. 2383, as amended, which is classified principally to chapter 9 (section 601 et seq.) of Title 41, Public Contracts. For complete classification of this Act to the Code see Short Title note set out under section 601 of Title 41 and Tables volume.

1986 Amendments. Subsec. (a). Pub.L. 99-500, Title I, § 101(m) [Title VIII, § 822(a)], designated existing provision as par. (1) and added pars. (2) and (3).

Pub.L. 99-591, Title I, § 101(m) [Title VIII, § 822(a)], made an amendment identical to Pub.L. 99-500, Title I, § 101(m) [Title VIII, § 822(a)].

Subsec. (b)(3). Pub.L. 99-500, Title I, § 101(m) [Title VIII, § 822(b)], added par. (3).

Pub.L. 99-591, Title I, § 101(m) [Title VIII, § 822(b)], made an amendment identical to Pub.L. 99-500, Title I, § 101(m) [Title VIII, § 822(b)].

Subsec. (c). Pub.L. 99-500, Title I, § 101(m) [Title VIII, § 821(b)(1)], struck out subsec. (c), which provided for the establishment of an automatic data processing fund, uses of the fund, and required an annual report on the fund be made to the Office of Management and Budget and Congress, and redesignated former subsec. (c) as (c).

Pub.L. 99-591, Title I, § 101(m) [Title VIII, § 821(b)(1)], made an amendment identical to Pub.L. 99-500, Title I, § 101(m) [Title VIII, § 821(b)(1)].

Subsec. (d). Pub.L. 99-500, Title I, § 101(m) [Title VIII, § 821(b)(1)], struck out subsec. (d), which related to the automatic data processing fund.

of net income to the Treasury at the close of each fiscal year, and redesignated former subsec. (f) as (d).

Pub.L. 99-591, Title I, § 101(m) [Title VIII, § 821(b)(1)], made an amendment identical to Pub.L. 99-500, Title I, § 101(m) [Title VIII, § 821(b)(1)].

Subsec. (e). Pub.L. 99-500, Title I, § 101(m) [Title VIII, § 821(b)(1)(B)], redesignated former subsec. (g) as (e). Former subsec. (c) redesignated (c).

Pub.L. 99-591, Title I, § 101(m) [Title VIII, § 821(b)(1)(B)], made an amendment identical to Pub.L. 99-500, Title I, § 101(m) [Title VIII, § 821(b)(1)(B)].

Pub.L. 99-591, Title I, § 101(m) [Title VIII, § 825], made an amendment identical to Pub.L. 99-500, Title I, § 101(m) [Title VIII, § 825].

Pub.L. 99-591, Title I, § 101(m) [Title VIII, § 823], made an amendment identical to Pub.L. 99-500, Title I, § 101(m) [Title VIII, § 823].

Pub.L. 99-500, Title I, § 101(m) [Title VIII, § 823], substituted "whether or not the automatic data processing equipment will be provided by the Administrator or whether or not the authority to lease, purchase, or maintain the equipment will be delegated" for "specifically affecting them or the automatic data processing equipment or components used by them" and substituted provision relating to review of a procurement denial by the Administrator and requiring that such review be on the basis of a written appeal for provision relating to review of a proposed determination, in the absence of mutual agreement between the Administrator and the agency or user concerned.

Pub.L. 99-500, Title I, § 101(m) [Title VIII, § 825], substituted "exercised by the Office of Management and Budget" for "exercised by the Bureau of the Budget".

Subsec. (f). Pub.L. 99-500, Title I, § 101(m) [Title VIII, § 821(b)(1)(B)], redesignated former

Pub.L. 99-591, Title I, § 101(m) [Title VIII, § 821(b)(1)(B)], made an amendment identical to Pub.L. 99-500, Title I, § 101(m) [Title VIII, § 821(b)(1)(B)].

Pub.L. 99-591, Title I, § 101(m) [Title VIII, § 824], made an amendment identical to Pub.L. 99-500, Title I, § 101(m) [Title VIII, § 824].

Pub.L. 99-500, Title I, § 101(m) [Title VIII, § 824], in par. (1) substituted "in connection with any procurement which is subject to this section" for "in connection with any procurement conducted under the authority of this section", "subject to delegation" for "conducted under delegations" and inserted provision that the authority of the board include authority to determine whether a procurement is subject to this section and authority to review regulations for consistency and providing that a proceeding, decision, or order not be subject to interlocutory appeal or review, and in par. (5)(A) inserted provision that the board may consider opinions of other federal agencies but not be bound by such opinions.

Subsec. (g). Pub.L. 99-500, Title I, § 101(m) [Title VIII, § 821(b)(1)(B)], redesignated former subsec. (i) as (g). Former subsec. (g) redesignated (e).

Pub.L. 99-591, Title I, § 101(m) [Title VIII, § 821(b)(1)(B)], made an amendment identical to Pub.L. 99-500, Title I, § 101(m) [Title VIII, § 821(b)(1)(B)].

Effective Date of 1986 Amendment. Amendment of subsecs. (a), (b), (e), and (f) of this section by sections 822, 823, 824, and 825 of Pub.L. 99-500 effective Oct. 18, 1986, and repeal of subsecs. (c) and (d) of this section and redesignation of subsecs. (e)-(i) as (c)-(g) by section 821(b)(1) of Pub.L. 99-500 effective Jan. 1, 1987, see section 833 of Title VIII of the Treasury, Postal Service, and General Government Appropriations Act, 1987 [Pub.L. 99-500, Title I, § 101(m), Oct. 18, 1986, 100 Stat. 1783-344; Pub.L. 99-591, Title I, § 101(m), Oct. 30, 1986, 100 Stat. 3341-344], set out as a note under section 757 of this title.

Effective and Termination Date of 1984 Amendment. Section 2713(b) of Pub.L. 98-369, which had directed that the amendment made by section 2713(a) of Pub.L. 98-369 [adding provisions of this section relating to the resolution of automatic data processing disputes] would cease to be effective on Jan. 15, 1988, was repealed by Pub.L. 99-500, Title I, § 101(m), [Title VIII, § 831], Oct. 18, 1986, 100 Stat. 1783-344; Pub.L. 99-591, Title I, § 101(m), Oct. 30, 1986, 100 Stat. 3341-344.

Computer Security Act of 1987. Sections 1, 2, and 5 to 8 of Pub.L. 100-235 provided that:

"Section 1. Short title.

"This Act [enacting sections 278g-3 and 278g-4 of Title 15, Commerce and Trade, amending this section and sections 272 and 278h of Title 15, and enacting provisions set out as a note under section 271 of Title 15] may be cited as the 'Computer Security Act of 1987'.

"Sec. 2. Purpose.

"(a) In general.—The Congress declares that improving the security and privacy of sensitive information in Federal computer systems is in the public interest, and hereby creates a means for

as for such systems, without limiting the scope of security measures already planned or in use.

"(b) Specific purposes.—The purposes of this Act [Pub.L. 100-235] are—

"(1) by amending the Act of March 3, 1901, to assign to the National Bureau of Standards [sections 271 to 278h of Title 15] responsibility for developing standards and guidelines for Federal computer systems, including responsibility for developing standards and guidelines needed to assure the cost-effective security and privacy of sensitive information in Federal computer systems, drawing on the technical advice and assistance (including work products) of the National Security Agency, where appropriate;

"(2) to provide for promulgation of such standards and guidelines by amending section 111(d) of the Federal Property and Administrative Services Act of 1949 [subsec. (d) of this section];

"(3) to require establishment of security plans by all operators of Federal computer systems that contain sensitive information; and

"(4) to require mandatory periodic training for all persons involved in management, use, or operation of Federal computer systems that contain sensitive information.

"Sec. 5. Federal computers system security training.

"(a) In general.—Each Federal agency shall provide for the mandatory periodic training in computer security awareness and accepted computer security practice of all employees who are involved with the management, use, or operation of each Federal computer system within or under the supervision of that agency. Such training shall be—

"(1) provided in accordance with the guidelines developed pursuant to section 20(a)(5) of the National Bureau of Standards Act (as added by section 3 of this Act) [section 278g-3(a)(5) of Title 15], and in accordance with the regulations issued under subsection (c) of this section for Federal civilian employees; or

"(2) provided by an alternative training program approved by the head of that agency on the basis of a determination that the alternative training program is at least as effective in accomplishing the objectives of such guidelines and regulations.

"(b) Training objectives.—Training under this section shall be started within 60 days after the issuance of the regulations described in subsection (c). Such training shall be designed—

"(1) to enhance employees' awareness of the threats to and vulnerability of computer systems; and

"(2) to encourage the use of improved computer security practices.

"(c) Regulations.—Within six months after the date of the enactment of this Act [Jan. 8, 1988], the Director of the Office of Personnel Management shall issue regulations prescribing the procedures and scope of the training to be provided Federal civilian employees under subsection (a) and the manner in which such training is to be carried out.

"Sec. 6. Additional responsibilities for computer

"(a) Identification of systems that contain sensitive information.—Within 6 months after the date of enactment of this Act [Jan. 8, 1988], each Federal agency shall identify each Federal computer system, and system under development, which is within or under the supervision of that agency and which contains sensitive information.

"(b) Security plan.—Within one year after the date of enactment of this Act [Jan. 8, 1988], each such agency shall, consistent with the standards, guidelines, policies, and regulations prescribed pursuant to section 111(d) of the Federal Property and Administrative Services Act of 1949 [subsec. (d) of this section], establish a plan for the security and privacy of each Federal computer system identified by that agency pursuant to subsection (a) that is commensurate with the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of the information contained in such system. Copies of each such plan shall be transmitted to the National Bureau of Standards and the National Security Agency for advice and comment. A summary of such plan shall be included in the agency's five-year plan required by section 3505 of title 44, United States Code [section 3505 of Title 44, Public Printing and Documents]. Such plan shall be subject to disapproval by the Director of the Office of Management and Budget. Such plan shall be revised annually as necessary.

"Sec. 7. Definitions.

"As used in this Act [Pub.L. 100-235], the terms 'computer system', 'Federal computer system', 'operator of a Federal computer system', 'sensitive information', and 'Federal agency' have the meanings given in section 20(d) of the National Bureau of Standards Act (as added by section 3 of this Act [section 278g-3(d) of Title 15]).

"Sec. 8. Rules of construction of Act.

"Nothing in this Act, or in any amendment made by this Act [Pub.L. 100-235], shall be construed—

"(1) to constitute authority to withhold information sought pursuant to section 552 of title 5, United States Code [section 552 of Title 5, Government Organization and Employees]; or

"(2) to authorize any Federal agency to limit, restrict, regulate, or control the collection, maintenance, disclosure, use, transfer, or sale of any information (regardless of the medium in which the information may be maintained) that is—

"(A) privately-owned information;

"(B) disclosable under section 552 of title 5, United States Code, or other law requiring

or authorizing the public disclosure of information; or

"(C) public domain information."

Legislative History. For legislative history and purpose of Pub.L. 99-591, see 1986 U.S. Code Cong. and Adm. News, p. 5927. See, also, Pub.L. 100-235, 1987 U.S. Code Cong. and Adm. News, p. 3120.

West's Federal Practice Manual

Bid protests, see § 1782.

Law Review Commentaries

A review of the first year of ADP bid protests at the GSBGA. John R. Tolle, 16 Pub.Cont.L.J. 120 (1986).

Notes of Decisions

Resolution of disputes

Generally 4

Presumption of contract validity 5

1. Data processing equipment within section

This section provides for election of mutually exclusive administrative forums regarding challenges to procurement of certain automatic data processing equipment support services. 1985, 65 Op.Comp.Gen. 72.

4. Resolution of disputes—Generally

General Services Administration Board of Contract Appeals has authority under statute [40 U.S.C.A. § 759(h)(5)(B)] to determine whether a contract award violates a statute or regulation and to modify, revoke or suspend procurement authority, but it does not sit to settle rights of a terminated contractor vis-a-vis the Government, a matter not litigated in protest nor within its protest jurisdiction; such matters must be resolved in the traditional forums for their resolution. U.S. v. Amdahl Corp., C.A.Fed.1986, 786 F.2d 387.

5. — Presumption of contract validity

Section of Federal Property and Administrative Services Act [40 U.S.C.A. § 759(h)(6)(B)], which provides a presumption of validity as to all goods or services delivered and accepted under a contract revoked, suspended, or revised by the General Services Administration Board of Contract Appeals, preserves existing precedent with respect to protecting contractors who have performed under a contract which is later "rescinded" by GSBGA; in a sense, it is a limitation on Board's authority in that Board may not force Government to undue all that has occurred. U.S. v. Amdahl Corp., C.A.Fed.1986, 786 F.2d 387.

CHAPTER 21—NATIONAL CAPITAL MEMORIALS AND COMMEMORATIVE WORKS

Sec.

1001. Purposes.

1002. Definitions.

1003. Congressional authorization of commemorative works; consultation with Nation-

Sec.

as; membership; duty to advise on policy and procedure.

1005. Availability of map for public inspection.

1006. Specific conditions applicable to Areas I and II.

COMPUTER SECURITY ACT OF 1987

P.L. 100-235, see page 101 Stat. 1724

DATES OF CONSIDERATION AND PASSAGE

House June 22, 1987

Senate December 21, 1987

House Report (Science, Space, and Technology Committee)
No. 100-153(I), June 11, 1987 [To accompany H.R. 145]

House Report (Government Operations Committee) No. 100-153(II),
June 11, 1987 [To accompany H.R. 145]

Cong. Record Vol. 133 (1987)

No Senate Report was issued with this legislation. The House
Report (Parts I, this page, and II, page 3157) and the Signing
Statement of the President (page 3197-1) are set out.

HOUSE REPORT NO. 100-153(I)

[page 1]

The Committee on Science, Space, and Technology, to whom was referred the bill (H.R. 145) to provide for a computer standards program within the National Bureau of Standards, to provide for Government-wide computer security, and to provide for the training in security matters of persons who are involved in the management, operation, and use of Federal Computer systems, and for other purposes, having considered the same, report favorably thereon with an amendment and recommend that the bill as amended do pass.

P.L. 100-235

[page 6]

I. BACKGROUND

Computers and information systems have so permeated today's society that there is virtually no sector which does not rely heavily on their use. This includes the Federal Government, which currently has over 17,000 medium- and large-scale computers and will have almost 500,000 microcomputers by 1990, according to a 1987 report by the General Services Administration, entitled "AI Management of Information Systems".

The Federal Government is the largest single user of computers in the world. Its investment in automated systems technology is large: about 1.6 percent of the 1986 budget was spent on automated data processing (ADP) equipment and services, or more than \$1.5 billion dollars. This budget included ADP for defense and national security, education, national energy programs, social welfare, and tax programs.

As the role of the Federal Government has become broader, the need to automate and the corresponding need to secure data has grown. In recent years, Congress and the executive agencies have directed their attention to Federal computer systems in a number of areas, including investigating and commenting on the integrity and security. Both Section 111(f) of the Federal Property and Administrative Service Act of 1949 (as amended by the Brooks Act of 1965) and the Paperwork Reduction Act of 1980 represent attempts by Congress to address the issues of automating information in Federal agencies and creating an efficient method of storing and disseminating this information. In October 1984, Congress passed the first Federal computer crime legislation, the Counterfeit Access Device and Computer Fraud Act of 1984 (P.L. 98-473). This law has been amended by the Computer Fraud and Abuse Act of 1986 (P.L. 99-474). This law prohibited "unauthorized access" to "Federal interest computers" affecting national security data, financial data, and other data stored in these computers. In addition, penalties were established for pirated "bulletin boards" containing

[page 7]

information which might lead to the fraud or abuse of data in a computer.

Within the Federal Government several agencies have been charged with the responsibility for establishing computer security controls and standards. The Office of Management and Budget (OMB) has overall responsibility for computer security policy. The General Services Administration (GSA) also issues regulations on the physical security of computer facilities, and ensures that security hardware and software meet certain technological and fiscal specifications. In defense and national security, the National Security

MEMORANDUM OF UNDERSTANDING
BETWEEN
THE DIRECTOR OF THE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
AND
THE DIRECTOR OF THE NATIONAL SECURITY AGENCY
CONCERNING
THE IMPLEMENTATION OF PUBLIC LAW 100-235

Recognizing that:

A. Under Section 2 of the Computer Security Act of 1987 (Public Law 100-235), (the Act), the National Institute of Standards and Technology (NIST) has the responsibility within the Federal Government for:

1. Developing technical, management, physical, and administrative standards and guidelines for the cost-effective security and privacy of sensitive information in Federal computer systems as defined in the Act; and,

2. Drawing on the computer system technical security guidelines of the National Security Agency (NSA) in this regard where appropriate.

B. Under Section 3 of the Act, the NIST is to coordinate closely with other agencies and offices, including the NSA, to assure:

1. Maximum use of all existing and planned programs, materials, studies, and reports relating to computer systems security and privacy, in order to avoid unnecessary and costly duplication of effort; and,

2. To the maximum extent feasible, that standards developed by the NIST under the Act are consistent and compatible with standards and procedures developed for the protection of classified information in Federal computer systems.

C. Under the Act, the Secretary of Commerce has the responsibility, which he has delegated to the Director of NIST, for appointing the members of the Computer System Security and Privacy Advisory Board, at least one of whom shall be from the NSA.

Therefore, in furtherance of the purposes of this MOU, the Director of the NIST and the Director of the NSA hereby agree as follows:



I. The NIST will:

1. Appoint to the Computer Security and Privacy Advisory Board at least one representative nominated by the Director of the NSA.
2. Draw upon computer system technical security guidelines developed by the NSA to the extent that the NIST determines that such guidelines are consistent with the requirements for protecting sensitive information in Federal computer systems.
3. Recognize the NSA-certified rating of evaluated trusted systems under the Trusted Computer Security Evaluation Criteria Program without requiring additional evaluation.
4. Develop telecommunications security standards for protecting sensitive unclassified computer data, drawing upon the expertise and products of the National Security Agency, to the greatest extent possible, in meeting these responsibilities in a timely and cost effective manner.
5. Avoid duplication where possible in entering into mutually agreeable arrangements with the NSA for the NSA support.
6. Request the NSA's assistance on all matters related to cryptographic algorithms and cryptographic techniques including but not limited to research, development, evaluation, or endorsement.

II. The NSA will:

1. Provide the NIST with technical guidelines in trusted technology, telecommunications security, and personal identification that may be used in cost-effective systems for protecting sensitive computer data.
2. Conduct or initiate research and development programs in trusted technology, telecommunications security, cryptographic techniques and personal identification methods.
3. Be responsive to the NIST's requests for assistance in respect to all matters related to cryptographic algorithms and cryptographic techniques including but not limited to research, development, evaluation, or endorsement.
4. Establish the standards and endorse products for application to secure systems covered in 10 USC Section 2315 (the Warner Amendment).

5. Upon request by Federal agencies, their contractors and other government-sponsored entities, conduct assessments of the hostile intelligence threat to federal information systems, and provide technical assistance and recommend endorsed products for application to secure systems against that threat.

III. The NIST and the NSA shall:

1. Jointly review agency plans for the security and privacy of computer systems submitted to NIST and NSA pursuant to section 6(b) of the Act.

2. Exchange technical standards and guidelines as necessary to achieve the purposes of the Act.

3. Work together to achieve the purposes of this memorandum with the greatest efficiency possible, avoiding unnecessary duplication of effort.

4. Maintain an ongoing, open dialogue to ensure that each organization remains abreast of emerging technologies and issues effecting automated information system security in computer-based systems.

5. Establish a Technical Working Group to review and analyze issues of mutual interest pertinent to protection of systems that process sensitive or other unclassified information. The Group shall be composed of six federal employees, three each selected by NIST and NSA and to be augmented as necessary by representatives of other agencies. Issues may be referred to the group by either the NSA Deputy Director for Information Security or the NIST Deputy Director or may be generated and addressed by the group, upon approval by the NSA DDI or NIST Deputy Director. Within 14 days of the referral of an issue to the Group by either the NSA Deputy Director for Information Security or the NIST Deputy Director, the Group will respond with a progress report and plan for further analysis, if any.

6. Exchange work plans on an annual basis on all research and development projects pertinent to protection of systems that process sensitive or other unclassified information, including trusted technology, technology for protecting the integrity and availability of data, telecommunications security and personal identification methods. Project updates will be exchanged quarterly, and project reviews will be provided by either party upon request of the other party.

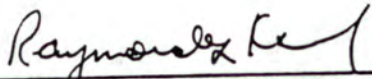
7. Ensure the Technical Working Group reviews prior to public disclosure all matters regarding technical systems security techniques to be developed for use in protecting sensitive information in federal computer systems to ensure they are

consistent with the national security of the United States. If NIST and NSA are unable to resolve such an issue within 60 days, either agency may elect to raise the issue to the Secretary of Defense and the Secretary of Commerce. It is recognized that such an issue may be referred to the President through the NSC for resolution. No action shall be taken on such an issue until it is resolved.

8. Specify additional operational agreements in annexes to this MOU as they are agreed to by NSA and NIST.

IV. Either party may elect to terminate this MOU upon six months written notice.

This MOU is effective upon approval of both signatories.



RAYMOND G. KAMMER
Acting Director
National Institute of
Standards and Technology



W. O. STUDEMAN
Vice Admiral, U.S. Navy
Director
National Security Agency

DATE: Mar 24, 1989

DATE: 23 March 1989

MILITARY AND CIVILIAN CONTROL OF COMPUTER
SECURITY ISSUES

HEARING
BEFORE THE
LEGISLATION AND NATIONAL SECURITY
SUBCOMMITTEE
OF THE
COMMITTEE ON
GOVERNMENT OPERATIONS
HOUSE OF REPRESENTATIVES
ONE HUNDRED FIRST CONGRESS
FIRST SESSION

MAY 4, 1989

Printed for the use of the Committee on Government Operations



COMMITTEE ON GOVERNMENT OPERATIONS

JOHN CONYERS, Jr., Michigan, *Chairman*

CARDISS COLLINS, Illinois	FRANK HORTON, New York
GLENN ENGLISH, Oklahoma	ROBERT S. WALKER, Pennsylvania
HENRY A. WAXMAN, California	WILLIAM F. CLINGER, Jr., Pennsylvania
TED WEISS, New York	AL McCANDLESS, California
MIKE SYNAR, Oklahoma	HOWARD C. NIELSON, Utah
STEPHEN L. NEAL, North Carolina	DONALD E. "BUZ" LUKENS, Ohio
DOUG BARNARD, Jr., Georgia	J. DENNIS HASTERT, Illinois
BARNEY FRANK, Massachusetts	JON L. KYL, Arizona
TOM LANTOS, California	CHRISTOPHER SHAYS, Connecticut
ROBERT E. WISE, Jr., West Virginia	PETER SMITH, Vermont
BARBARA BOXER, California	STEVEN SCHIFF, New Mexico
MAJOR R. OWENS, New York	CHUCK DOUGLAS, New Hampshire
EDOLPHUS TOWNS, New York	LARKIN I. SMITH, Mississippi
JOHN M. SPRATT, Jr., South Carolina	C. CHRISTOPHER COX, California
JOE KOLTER, Pennsylvania	CRAIG THOMAS, Wyoming
BEN ERDREICH, Alabama	
GERALD D. KLECZKA, Wisconsin	
ALBERT G. BUSTAMANTE, Texas	
MATTHEW G. MARTINEZ, California	
LOUISE M. SLAUGHTER, New York	
NANCY PELOSI, California	
DONALD M. PAYNE, New Jersey	
JIM BATES, California	

JULIAN EPSTEIN, *Staff Director*
DONALD W. UPSON, *Minority Staff Director*

LEGISLATION AND NATIONAL SECURITY SUBCOMMITTEE

JOHN CONYERS, Jr., Michigan, *Chairman*

STEPHEN L. NEAL, North Carolina	FRANK HORTON, New York
BEN ERDREICH, Alabama	ROBERT S. WALKER, Pennsylvania
GERALD D. KLECZKA, Wisconsin	JON L. KYL, Arizona
GLENN ENGLISH, Oklahoma	CHRISTOPHER SHAYS, Connecticut
BARBARA BOXER, California	
ALBERT G. BUSTAMANTE, Texas	

RICHARD C. BARNES, *Staff Director*
THOMAS A. TRIMBOLI, *Counsel*
BENNIE WILLIAMS, *Clerk*
GREGORY KILGORE, *Minority Professional Staff*

(III)

CONTENTS

	Page
Hearing held on May 4, 1989.....	1
Statement of:	
Adler, Allan R., Esq., attorney, Cohn & Marks.....	181
Allen, Kenneth, senior vice president, government relations, Information Industry Association, Washington, DC.....	141
Belisle, Albert R., vice chairman, Information Systems Security Management Committee, American Bankers Association	154
Berman, Jerry J., director, Information Technology Project, American Civil Liberties Union	54
Brooks, Hon. Jack, a Representative in Congress from the State of Texas, and chairman, Committee on the Judiciary.....	5
Conyers, Hon. John, Jr., a Representative in Congress from the State of Michigan, and chairman, Legislation and National Security Subcommittee: Opening statement	1
Courtney, Robert H., Jr., president, RCI, Inc	171
Drake, Miriam A., director of libraries, Georgia Institute of Technology, on behalf of the American Library Association and the Association of Research Libraries	120
Glickman, Hon. Dan, a Representative in Congress from the State of Kansas	12
Hearn, Dr. James J., Deputy Director for Information Security, National Security Agency, accompanied by Elizabeth Rindskopf, General Counsel	193
Hoffman, Lance J., professor of electrical engineering and applied science, George Washington University	130
Kammer, Raymond, Acting Director, National Institute of Standards and Technology	219
Rotenberg, Marc, director, Washington office, Computer Professionals for Social Responsibility	80
Socular, Milton J., Special Assistant to the Comptroller General, U.S. General Accounting Office, accompanied by Jack L. Brock, Jr., Director, Government Information and Financial Management Issues.....	36
Letters, statements, etc., submitted for the record by:	
Adler, Allan R., Esq., attorney, Cohn & Marks: Prepared statement.....	183-192
Allen, Kenneth, senior vice president, government relations, Information Industry Association, Washington, DC: Prepared statement.....	143-153
Belisle, Albert R., vice chairman, Information Systems Security Management Committee, American Bankers Association: Prepared statement	156-170
Berman, Jerry J., director, Information Technology Project, American Civil Liberties Union: Prepared statement	57-79
Brooks, Hon. Jack, a Representative in Congress from the State of Texas, and chairman, Committee on the Judiciary: Prepared statement.....	8-11
Conyers, Hon. John, Jr., a Representative in Congress from the State of Michigan, and chairman, Legislation and National Security Subcommittee:	
Material submitted for the hearing record	288-316
Memorandum of understanding between Director of the National Institute of Standards and Technology and Director of the National Security Agency re implementation of Public Law 100-235	24-27
Courtney, Robert H., Jr., president, RCI, Inc.: Prepared statement	174-180
Drake, Miriam A., director of libraries, Georgia Institute of Technology, on behalf of the American Library Association and the Association of Research Libraries: Prepared statement.....	121-129

(III)

Letters, statements, etc., submitted for the record by—Continued

Glickman, Hon. Dan, a Representative in Congress from the State of Kansas: Prepared statement	15-22
Hearn, Dr. James J., Deputy Director for Information Security, National Security Agency: Prepared statement	195-208
Hoffman, Lance J., professor of electrical engineering and applied science, George Washington University: Prepared statement	132-137
Horton, Hon. Frank, a Representative in Congress from the State of New York:	
Correspondence relative to the hearing	215-218
May 2, 1989, article from the Washington Post, entitled "FBI May Release Library-Probe Files"	139
Kammer, Raymond, Acting Director, National Institute of Standards and Technology: Prepared statement	221-282
Rotenberg, Marc, director, Washington office, Computer Professionals for Social Responsibility: Prepared statement	83-119
Socular, Milton J., Special Assistant to the Comptroller General, U.S. General Accounting Office:	
Prepared statement	39-47
Responses to subcommittee questions	50-53

MILITARY AND CIVILIAN CONTROL OF COMPUTER SECURITY ISSUES

THURSDAY, MAY 4, 1989

HOUSE OF REPRESENTATIVES,
LEGISLATION AND NATIONAL SECURITY SUBCOMMITTEE
OF THE COMMITTEE ON GOVERNMENT OPERATIONS,
Washington, DC.

The subcommittee met, pursuant to notice, at 10:07 a.m., in room 2154, Rayburn House Office Building, Hon. John Conyers, Jr. (chairman of the subcommittee) presiding.

Present: Representatives John Conyers, Jr., Gerald D. Kleczka, Glenn English, Frank Horton, Jon L. Kyl, and Christopher Shays.

Also present: Representative Jim Bates.

Staff present: Thomas A. Trimboli, counsel; and Gregory Kilgore, minority professional staff, Committee on Government Operations.

OPENING STATEMENT OF CHAIRMAN CONYERS

Mr. CONYERS. The subcommittee will come to order. This morning we will review the manner in which the Department of Commerce and its National Institute on Standards and Technology are planning to execute their respective functions under the Computer Security Act of 1987.

[The opening statement of Mr. Conyers follows:]

(1)

PREPARED TESTIMONY
AND
STATEMENT FOR THE RECORD

OF

MARC ROTENBERG
DIRECTOR, WASHINGTON OFFICE

COMPUTER PROFESSIONALS FOR
SOCIAL RESPONSIBILITY (CPSR)

ON

THE COMPUTER SECURITY ACT OF 1987 (P.L. 100-235)
AND THE MEMORANDUM OF UNDERSTANDING BETWEEN
THE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST)
AND THE NATIONAL SECURITY AGENCY (NSA)

BEFORE

THE SUBCOMMITTEE ON LEGISLATION AND NATIONAL SECURITY,
COMMITTEE ON GOVERNMENT OPERATIONS

U.S. HOUSE OF REPRESENTATIVES

MAY 4, 1989

Mr. Chairman, members of the Committee, thank you for the opportunity to testify today on the implementation of the Computer Security Act. I am testifying on behalf of Computer Professionals for Social Responsibility (CPSR), a national membership organization of computer scientists. CPSR has reviewed a number of federal computing proposals, including a detailed assessment of the proposed expansion of the FBI's record system for Congressman Don Edwards.

I would like to thank you for convening this hearing. In our letter to the Committee earlier this month, we emphasized that vigorous oversight would be necessary for successful implementation of the Computer Security Act. We are very pleased that you have undertaken this hearing.

You have asked me to review the Memorandum of Understanding between NIST and NSA and to determine whether it complies with the spirit and intent of the Computer Security Act.¹ To answer that question it is necessary to look at the history of the Act and the record established by this Committee.

THE IMPORTANCE OF THE COMPUTER SECURITY ACT

The central computer security question in the last two Congresses was whether responsibility for the security and privacy

¹ "Memorandum of Understanding Between the Director of the National Institute of Standards and Technology and the Director of the National Security Agency Concerning the Implementation of Public Law 100-235" (signed March 23, 1989); Public Law No. 100-235, 1988 U.S. Code Congressional and Administrative News (100 Stat.) 1724.

of information stored in government computer systems should be entrusted to a civilian agency or an intelligence agency.

In 1984, the President had issued a National Security Decision Directive, NSDD-145, which gave the intelligence agencies broad authority to peruse computer databases, for so-called "sensitive but unclassified information."² A subsequent memorandum from John Poindexter, expanded this authority still further to include "all computer and communications security for the Federal Government and private industry."³ As the government's authority to control access to computerized information for the purpose of protecting national security expanded, the free flow of information diminished.⁴ Stories of agents visiting private information vendors and public libraries soon followed.⁵ At the same time, a wide range of other

² "National Policy on Telecommunications and Automated Information Systems Security" (September 17, 1984).

³ The memorandum, NTISSP No. 2 "Policy for Protection of Sensitive, but Unclassified Information in Federal Government Telecommunications and Automated Systems," was eventually rescinded. David Sanger, "Rise and Fall of U.S. Data Directive," The New York Times, March 19, 1987.

⁴ See generally Jerry J. Berman, "National Security vs. Access to Computer Databases: A New Threat to Freedom of Information," 2 Software Law Journal 1 (1987).

⁵ Bob Davis, "Federal Agencies Press Data-Base Firms to Curb Access to 'Sensitive' Information," The Wall Street Journal, January 28, 1987; Judith Axler Turner, "Pentagon Planning to Restrict Access to Public Data Bases," The Chronicle of Higher Education, January 21, 1987; Connie Oswald Stofko, "Inquiry by FBI Causes Libraries to Assess Records," SUNY Reporter, February 12, 1987. The NSA also approached election officials and investigated computerized vote-counting software. Burnham, "US Examines if

activities by the government further threatened to restrict access to information.⁶

Many organizations opposed these efforts. Mead Data Central warned that such "restrictive and unwarranted policies" threatened not only the information industry, but many sectors of the economy, "including legal, financial, government, medical, and the scientific and technological community."⁷ The IEEE stated that the "unabridged dissemination of unclassified scientific and technical information is crucial for the continued advancement of US industry."⁸ The American Bankers Association expressed concern that NSA encryption technologies would be ill-suited for the private sector and criticized the failure of NSA to recertify the

Computer Used in '84 Elections is Open to Fraud," The New York Times, September 24, 1985, at A17.

⁶ See American Library Association, Less Access to Less Information by and about the U.S. Government (1988); Steven L. Katz, "National Security Controls, Information, and Communications in the United States," 4 Government Information Quarterly 63 (1987); People For the American Way, Government Secrecy: Decisions without Democracy (1987); John Shattuck & Muriel Morisey Spence, Government Information Controls: Implications for Scholarship, Science and Technology, excerpted in "When Government Controls Information," 91 Technology Review 62 (April 1988).

⁷ House Committee on Science, Space, and Technology, H.R. Rep. No. 153, pt. 1, 100th Cong., 1st Sess. 18 (1987) [the "Science Committee Report"], reprinted in 1988 U.S. Code Congressional and Administrative News 3133 ["1988 U.S.C.A.N."] (Statement of Jack W. Simpson, President, Mead Data Central).

⁸ Science Committee Report at 19, reprinted in 1988 U.S.C.A.N. 3134 (statement of John M. Richardson, Chairman, Committee on Communications and Information Policy, Institute of Electrical and Electronic Engineering).

public key cryptography standard DES.⁹ The American Library Association identified a threat to intellectual freedom and adopted a resolution calling for the repeal of the new security directive.¹⁰ And Jerry Berman, with the ACLU, in testimony before this Committee, warned of the dangers of unleashing the NSA to patrol computers. He said:

There are good reasons for current limitations and why we should worry about whether they are being eroded by NSDD-145. NSA operates outside the normal accountability channels which control other agencies of government. It has no legislated charter. Its existence was not acknowledged until 1962.¹¹

This Committee, already in the process of reviewing federal computer standards, made clear its opposition to the NSA's activities, through letters, statements, and a comprehensive hearing record. Chairman Brooks said that NSDD-145 was "one of the most ill-advised and potentially troublesome directives ever issued by a President" and warned that a new form of government censorship would result if a secret intelligence agency was responsible for computer security throughout the federal

⁹ Computer Security Act of 1987: Hearings on H.R. 145 Before a Subcommittee of the Committee on Government Operations, House of Representatives, 100th Cong., 1st Sess. 113-14 [the "Hearings"] (statement of Cheryl W. Helsing), Science Committee Report at 19, reprinted in 1988 U.S.C.A.N. 3133.

¹⁰ Id. at 550-51.

¹¹ Hearings at 104. See generally U.S. Senate, Select Committee to Study Governmental Operations with Respect to Intelligence Agencies (1976), James Bamford, The Puzzle Palace (1983), David Burnham, The Rise of the Computer State 118-44 (1983), Morton H. Halperin, Jerry J. Berman, et al., The Lawless State 171-86 (1976)

government.¹² Congressman Glickman, the sponsor of the bill which became the Computer Security Act, stated that there was a fundamental problem with "any directive that affected virtually all civil agencies of government and that had been issued without any public comment."¹³ Congressman English stressed that the "insatiable desire of the military for controlling information" was the most convincing argument for legislation.¹⁴

In short, there was a widely shared belief, based on experience and public policy considerations, that the National Security Agency was the wrong agency to set computer security standards for the federal government.

In passing the Computer Security Act, Congress decided that a civilian agency, the National Institute of Standards and Technology, would be responsible for computer security. NIST was already authorized under the Brooks Act to set standards for computer systems, and had been working on computer standards since the early 1960s when it helped develop the widely used encryption program, DES. And, unlike the NSA, NIST had a good reputation with the private sector.¹⁵

Congress recognized that there were computer systems operated

¹² Hearings at 525, 526.

¹³ Id. at 456.

¹⁴ Id. at 23.

¹⁵ Id. at 320, reprinted in Government Operations Committee Report at 12, reprinted in 1988 U.S.C.A.N. 3164 (statement of Robert H. Courtney).

in military and intelligence agencies that may pose special or unique problems, requiring NSA technical guidelines. But Congress went to great lengths to spell out these systems, citing statutes, detailing procedures, and avoiding such phrase as "sensitive but unclassified," or "national security," that were overly broad or easily misconstrued.

Thus, on the central question of which agency was responsible for computer security in the federal government, the intent of Congress is unambiguous; the Act stated that "the National Bureau of Standards shall have the mission of developing standards, guidelines, and associated methods and techniques for computers systems."¹⁶

Since the passage of the Act, NIST has been working to implement the requirements of the Act, reviewing agency security plans, conducting open meetings, and initiating research on computer standards.¹⁷ About a month ago, NIST and NSA signed a Memorandum of Understanding. The central question before the Committee now is whether the M.O.U. is consistent with the Act passed by Congress and signed by the President.

INCONSISTENCIES BETWEEN THE M.O.U. AND THE COMPUTER SECURITY ACT

A Memorandum of Understanding between two agencies should

¹⁶ § 3, 15 U.S.C. § 278g-3(a)(1).

¹⁷ Kevin Power, "NIST Sets Security Review Deadline," Government Computer News, November 21, 1988, at 97; Kevin Power, "Analysts Prepare to Review Agency Security Plans," Government Computer News, January 9, 1989, at 81.

clarify the responsibilities of each agency, the methods in which each agency will undertake its assignments, in a manner that is consistent with the authorizing legislation. The M.O.U. fails this threshold test.

- It transfers the authority to establish and review computer standards from the NIST to the NSA;
- It undermines the authority of the Advisory Board, established by the Act;
- It creates a new layer of national security review;
- It invites the NSA to enter the offices of private information companies and government contractors;
- It revives many of the problems arising from the phrase "sensitive but unclassified";
- It grants NSA the opportunity to review all matters of cryptography undertaken by NIST.

Instead of resolving issues left open by the Act, such as the status of NSDD-145, it undermines the Act, transferring authority that Congress intended to remain at the Commerce Department to Fort Meade.

Under the Act, Congress made clear that NIST would be responsible for federal computer security. The language is straightforward and consistent. The preamble states: "To provide for a computer standards program within the National Bureau of

Standards."¹⁸ The amendments to the NIST organic act say: "The National Bureau of Standards shall have the mission of developing standards, guidelines and associated methods and techniques for computer systems;"¹⁹ the NIST has "the responsibility within the Federal Government for developing . . . standards and guidelines for the cost effective security and privacy of sensitive information in Federal computer systems."²⁰ The amendments to the Brooks Act state that:

The Secretary of Commerce shall, on the basis of Standards and guidelines developed by that National Bureau of Standards . . . promulgate standards and guidelines pertaining to federal computer systems, making such standards compulsory and binding to the extent to which the Secretary determines necessary to improve the efficiency of operation or security and privacy of Federal computer systems.²¹

NSA was given an advisory role, to offer "technical advice and assistance," where appropriate.²² NSA retained authority only over those computer systems that were exempted under the statute. These systems were indicated explicitly by reference to statute or

¹⁸ The Computer Security Act, preamble, 101 Stat. 1724 (1988).

¹⁹ Id. § 3, 15 U.S.C. § 278g-3(a)(1).

²⁰ Id. § 3, 15 U.S.C. § 278g-3(a)(3).

²¹ Id. § 4, 40 U.S.C. § 759 note.

²² Id. § 4, 40 U.S.C. § 759 note. See id. § 3, 15 USC § 278g-3(c)(2).

to established procedures specifically authorized under criteria established by Executive order or an act of Congress.²³

In passing the Computer Security Act, Congress did not create a joint venture. The NSA is one of many agencies that is expected to work with NIST to help implement the Act. Under the Act, NIST is authorized to coordinate closely with other agencies, including the Departments of Defense and Energy, the General Accounting Office, the Office of Technology Assessment, and the Office of Management and Budget.²⁴ The Office of Personnel Management is also required to issue regulations prescribing the procedures for computer system security training, based on guidelines developed by NIST.²⁵

The Administration, in endorsing passage of the Computer Security Act, also made clear that it expected NIST to be responsible for computer standards and for NSA to provide assistance, as NIST saw fit. A letter from OMB Director Jim Miller stated that:

²³ See id. § 3, 15 U.S.C. 278g-3(a) (3)

²⁴ Id. § 3.

²⁵ Id. § 6, 40 U.S.C. 759 note.

Computer security standards, like other computer standards, will be developed in accordance with established NBS procedures. In this regard the technical security guidelines provided by NSA to NBS will be treated as advisory and subject to appropriate, NBS review.²⁶

But the M.O.U. cedes NIST standard-setting authority to the NSA. Instead of providing technical advice and assistance, as required by the Act, NSA is now setting the rules. The M.O.U. requires NIST to recognize "the NSA-certified rating of evaluated trusted systems under the Trusted Computer Security Evaluation Criteria without requiring additional evaluation."²⁷ This is the so-called Orange Book, developed by the NSA, that sets out the different levels of security for computer systems.

This Committee and witnesses who testified at the hearings raised serious doubts about the Orange Book.²⁸ The Office of Technology Assessment also questioned whether the Orange Book standards would be appropriate for the diverse needs of the federal government.²⁹ In fact, these guidelines could be fundamentally at odds with our system of open government.

²⁶ Government Operations Committee Report at 37, reprinted in 1988 U.S.C.A.N. 3189 (letter to Congressman Brooks); Science Committee Report at 41, reprinted in 1988 U.S.C.A.N. 3151 (letter to Congressman Roe).

²⁷ The M.O.U. at 2.

²⁸ Government Operations Committee Report at 26, reprinted in 1988 U.S.C.A.N. 3178. "Their guidance is not even accepted by the major data processing operations within NSA," Hearings at 313-21 (statement of Robert Courtney).

²⁹ Office of Technology Assessment, Defending Secrets, Sharing Data 117-127 (1987) (Charles K. Wilk, Project Director) [the "OTA Report"].

According to a paper titled "A Comparison of Commercial and Military Computer Security Policy," cited in the OTA Report, "military security policy is really a set of policies designed to control classified information from unauthorized disclosure or declassification."³⁰

Have those concerns been answered? Has NIST made a determination that the Orange book standards are consistent with the needs of civilian agencies? Is there a publicly reviewable record that explains the basis for this decision? Does the Advisory Board endorse this outcome?

More surprising is that the M.O.U. restricts the NIST from any prospective review of computer security standards. This provision is not only at odds with the intent of the Act, but will undermine efforts to enhance computer security. Innovation is critical for the development of new information security technologies.³¹

There is a legitimate concern about the development of different computer standards for federal computer systems. Congress recognized that it could be inefficient and costly. Computer manufacturers also did not want to develop computer

³⁰ OTA Report at 117, citing David D. Clark, MIT Laboratory for Computer Science, and David R. Wilson, Ernst & Whinney.

³¹ OTA Report at 6. This provision also suggests the cost that secrecy imposes on scientific innovation. See, e.g., Robert L. Park, "Science and Secrecy," Bulletin of Atomic Scientists, March, 1985, at 22. See Harold Willenbock, "Information Controls and Technological Progress," Issues in Science and Technology, Fall 1986, at 88. See generally National Academy of Sciences, Scientific Communications and National Security (1982)

systems for the federal government with two different sets of standards. For this reason the Act required that standards NIST developed be "consistent and compatible" with existing standards for the protection of properly classified systems.³² But Congress considered and explicitly rejected the proposition that NSA should have authority for developing technical guidelines:

Since work on technical security standards represents virtually all of the research effort being done today, NSA would take over virtually the entire computer standards from the National Bureau of Standards. By putting NSA in charge of developing technical security guidelines (software, hardware, communications), NBS would be left with the responsibility for only administrative and physical security measures -- which have generally been done years ago. NBS, in effect, would on the surface be given the responsibility for the computer standards program with little to say about the most important part of the program -- the technical guidelines developed by NSA.³³

It was clearly not the intent of Congress that NIST should become a clearinghouse for NSA's technical standards.

Second, the M.O.U. will undermine the Computer System Security and Privacy Advisory Board established by the Act. This Advisory Board is responsible for identifying emerging issues, advising NIST and the Secretary of Commerce, and reporting its findings to Commerce, OMB, NSA, and the Oversight Committees.³⁴

³² § 3, 15 U.S.C. § 278g-3(b) (6) (B).

³³ Government Operations Committee Report at 25-26, reprinted in 1988 U.S.C.A.N. 3177-78. See also Science Committee Report at 27, reprinted in 1988 U.S.C.A.N. 3142.

³⁴ § 3, 15 U.S.C. § 278g-4(b) (duties).

Under the Act, the Board is made up of leading representatives from the computer and telecommunications industry, the federal government and independent contractors; the Secretary of Commerce selects the Chair of the Board.³⁵ The purpose of the Board is to ensure that NIST "receives qualified input from those likely to be affected by its standards and guidelines, both in government and the private sector."³⁶ The American Bankers Association testified that "one of the most important aspects" of the bill "is the establishment of a formal mechanism for private sector communication and cooperation with the Federal Government."³⁷

The M.O.U. sets forth a different mechanism. It is a Technical Working Group that will review computer security issues.³⁸ It is headed by the NSA Deputy Director for Information Security and the NIST Deputy Director. Nowhere, in the M.O.U., is the relationship between the Working Group and the Advisory Board described.

There are three potential problems with this procedure. First, it is likely to divert issues to the Technical Working Group that should properly be considered by the Advisory Group. Second, creating a joint NSA-NIST committee for matters involving

³⁵ § 3, 15 U.S.C. § 278g-4(a).

³⁶ Science Committee Report at 27, reprinted in 1988 U.S.C.A.N. 3142. See also Government Operations Committee Report at 40, reprinted in 1988 U.S.C.A.N. 3192.

³⁷ Hearings at 114 (statement of Cheryl W. Helsing).

³⁸ The M.O.U. at 3-4.

unclassified computer systems is inconsistent with the roles assigned NIST and NSA under the Act. Third, because of the authority granted to the NSA Deputy Director under the M.O.U., the NSA could easily control the agenda of this working group. In effect, the M.O.U. allows NSA to refer any issue at any time to the working group for resolution within 14 days. This is simply not a sensible way to ensure NIST authority when the resources of NSA far exceed NIST.

Third, the M.O.U. creates a new layer of national security review. Under the M.O.U., "all matters regarding technical systems security techniques" must be reviewed, prior to public disclosure, to ensure that they are consistent with "national security."³⁹ In the words of Chairman Brooks, this procedure will shift decisions about computer security standards to "the basement of the White House and the back rooms of the Pentagon."⁴⁰

The framers of the Act provided a mechanism for review, but after the rules had been made public. This was purposeful. It was intended to avoid pre-publication review, and to strengthen the wall protecting the decision-making authority of the Commerce Department so as to prevent the national security administration from crawling in over the top. The procedure in the M.O.U. for National Security Council review effectively dismantles this safeguard.

³⁹ Id.

⁴⁰ Hearings at 2.

Fourth, the M.O.U. breathes new life into NSDD-145.

According to the M.O.U., the NSA will:

Upon request by Federal agencies, their contractors and other government-sponsored entities, conduct assessments of the hostile intelligence threat to federal information systems, and provide technical assistance and recommend endorsed products for application to secure systems against the threat.⁴¹

This is NSDD-145, part two. Will it have Congressional blessing? This language invites the National Security Agency back into the offices of information vendors to provide government security systems or to restrict access to electronic information. This was one of the key concerns that led to adoption of the Computer Security Act.⁴² Recall the statement of Assistant Secretary of Defense Donald Latham, chairman of NTISSC, who said:

I'm very concerned about what people are doing--and not just the Soviets. If that means putting a monitor on NEXIS type systems, I'm for it. The question is, how do you do that technically without interference?⁴³

The private sector responded that it was not the Kremlin they worried about, but their business competitors. But the M.O.U. resurrects the "hostile intelligence threat"⁴⁴ and leaves open the possibility that the government may very well put monitors on

⁴¹ The M.O.U. at 3.

⁴² See, e.g., "Are Data Bases a Threat to National Security?" *BusinessWeek*, December 1, 1986, at 39.

⁴³ *The Washington Post*, May 27, 1986.

⁴⁴ The M.O.U. at 3.

computer systems.

There is another aspect of this clause that is troubling. While it seems to restrict the ability for the NSA to visit purely "private" companies, it leaves open the possibility that any federal agency could request that the NSA undertake an assessment of any information system maintained by a federal contractor. Such a procedure will undercut NIST's authority for computer security and could be an open license for government surveillance of computer systems throughout the country.

The Act created a mechanism for the NSA to raise national security concerns. An NSA representative serves as a member of the Advisory Board. That is the appropriate place to discuss these questions.

Fifth, the efforts that Congress made to delineate the computer systems covered under the Act are largely swept aside by the language of the M.O.U.. In drafting the Act, Congress purposefully rejected the phrase "sensitive, but unclassified" and avoided the term "national security," fearing that this term would confuse the responsibilities of the NIST and the NSA. It used the term "public interest" to describe the President's authority to reject standards. It exempted from the Act those systems where information must be kept secret in the interest of "national defense" or "foreign policy." In part, and in whole, these choices show the determination of Congress to avoid the open-ended

trap of national security designations.⁴⁵ However, the M.O.U. ignores these decisions by Congress and says flatly that all systems must be reviewed to "ensure they are consistent with the national security of the United States."⁴⁶

It is also important to understand how the critical term "sensitive" is used in the Act. It does not create another category of restricted information.⁴⁷ It is used to underscore the importance of the information, and the risks that might result, such as loss of life or violation of personal privacy, if the information were modified, destroyed or disclosed.⁴⁸ In effect, it was to operate as a triggering mechanism, to help agency administrators distinguish between systems that might contain records on individuals and systems that were designed to be widely accessible, such as computerized bulletin boards.

The M.O.U. distorts this view of information protection and returns to the "sensitive but unclassified" approach of NSDD-145 and the Poindexter memorandum. It treats sensitive information as information that must be controlled, for which access may be restricted. This is how information security is viewed by

⁴⁵ See Harold C. Relyea, "National Security and Information," 4 Government Information Quarterly 11 (1987).

⁴⁶ The M.O.U. at 3-4.

⁴⁷ Government Operations Committee Report at 24, 31, reprinted in 1988 U.S.C.A.N. 3176, 3183.

⁴⁸ Science Committee Report at 21, reprinted in 1988 U.S.C.A.N. 3136.

intelligence agencies.⁴⁹ This approach to computer security could drape the entire federal government under a veil of national security review.

This is not simply at odds with the Computer Security Act, but also with the Freedom of Information Act, the law which establishes a fundamental right for citizens in the United States to have access to the records of government. It is the statute that preserves our open system of government and prevents the government from erecting barriers against its citizens. Congress anticipated this problem and added a section to the bill to make sure that computer security legislation would not erode the principles underlying the Freedom of Information Act.⁵⁰

A final question Mr. Chairman, what exactly did NIST and the NSA intend to accomplish by adoption of this M.O.U.? Presumably, it was to ensure the faithful compliance with Act. But even this is not clear. The M.O.U. states that NIST and the NSA will:

Work together to achieve the purposes of the memorandum with the greatest efficiency possible, avoiding unnecessary duplication of effort.⁵¹

If this M.O.U. is the basis for NIST-NSA cooperation for computer security, then the starting point must be a commitment to work

⁴⁹ See OTA Report at 117.

⁵⁰ § 8. See also statement of the President, 24 Weekly Compilation of Presidential Documents 10, January 11, 1988, reprinted in 1988 U.S.C.A.N. 3197-1 (January 8, 1988).

⁵¹ The M.O.U. at 3 [emphasis added].

together to achieve the purposes of the Act, as passed by Congress.

As it currently stands, the M.O.U. is directly at odds with the plain language of the Computer Security Act. Is this significant? Could the Committee simply say: that's not really what we intended, but, in comparison to NSDD-145, "sensitive but unclassified," and some of the other problems that led to passage of the Act, this may not be so pressing. The answer to that question is no. If it was important to pass the legislation, then it is important to see that it is implemented as Congress intended.

THE CONSEQUENCES OF IMPLEMENTING THE M.O.U.

The Memorandum of Understanding will have significant consequences for both the free flow of information and the type of security protection established by the federal government.

A. Impact on Access to Information

Less than three years ago, the Director for Information Systems for the Department of Defense, said:

I don't believe that the issue is whether or not we're going to protect information, I believe that the issue is what information we're going to protect both within the Federal Government, both within DOD and also within industry.⁵²

I believe, after reviewing the M.O.U., that NSA intends to make good on its promise. If left in place, this M.O.U. will restrict access to information for Congress, for information vendors and government contractors, and for the general public.

1. The Congress

Congress will require access to particular information about the conduct of the agencies to assess the program, and to determine when changes are necessary, and to appropriate adequate funds to get the job done. Without adequate oversight, there can be no assurance that the goals of the act will be achieved.

But if the Technical Working Group is left in place, then Congress may be denied access to information necessary to assess the progress of computer security. Under the M.O.U., the NSA will be able to appeal any proposed standards to the National Security Council, prior to publication. What happens when the NSC rules that certain standards may not be adopted? How will Congress find out? Under the Act, there is a clear mechanism for notifying the oversight committees if the President rejects a standard.⁵³

⁵² Government Operations Committee Report at 15, reprinted in 1988 U.S.C.A.N. 3167. "Are Data Bases a Threat to National Security?" *BusinessWeek*, December 1, 1986, at 39.

⁵³ § 4, 40 U.S.C. § 759(d) (1).

Absent a similar procedure for the Technical Working Group, this preliminary review may place the whole process of developing computer standards for the federal government behind the drawn curtain of national security.

2. Impact on Information Vendors and Government Contractors

Mead Data Central is one of the largest vendors of computer-based information in the world. It has over 200,000 customers and maintains more than 47 million full-text documents. Yet, in 1987, Mead Data Central reported to this Committee that it had removed the National Technical Institute Service (NTIS) file from its system. Although it cited economic and policy reasons for the decision, it is hard to escape the conclusion that, but for the pressure brought to bear by NSDD-145, that service would be available today.

What will happen when a smaller information vendor, a government contractor, or a government-sponsored organization, is approached by officials from Ft. Meade, notified of a potential hostile intelligence threat, and asked whether it would like NSA's assistance in improving computer security? What databases will then be removed? And how will Congress or anyone else know about actions taken by intelligence agencies under the banner of "national security"?

3. Impact on the public

The impact on the public of government restrictions on access to information has been widely documented.⁵⁴ Efforts to expand national security authority chill speech, restrict intellectual inquiry, hinder economic trade, constrain scientific innovation, and undermine open government.

If, under the M.O.U., the Congress is not able to obtain the information necessary to oversee the Act and information companies face possible new restrictions, what is the likely impact on the free flow of information for the general public? That is, of course, the central test for the implementation of the Act.

B. Impact on Protection of Information

Considering the history of NSDD-145 and the Poindexter memo,⁵⁵ the potential impact of the M.O.U. on the free flow of information is one way to assess whether the M.O.U. should be left unchanged; the other is whether the M.O.U. will establish security and privacy practices consistent with the Act.

The security goals of a civilian agency are often different than those of a military agency.⁵⁶ Emphasizing the computer security interest, as defined by the National Security Agency, could, in fact, undermine both the management goals and the privacy interests the Act seeks to protect.

⁵⁴ See note 6 and accompanying text.

⁵⁵ See notes 2-14 and accompanying text.

⁵⁶ See notes 29-31 and accompanying text.

Effective computer security plans should be built around solid-management practices, not gold-plated technologies. In a report for Congressman Don Edwards on the proposed expansion of the FBI's record system, CPSR members wrote:

Advances in computer technology can be used to improve security, accountability, and data quality. But system administrators and managers carry the ultimate responsibility to ensure that the system is well designed and properly maintained.⁵⁷

Technical guidelines should follow from organizational requirements. But shifting authority from NIST to NSA may undermine this fundamental goal of information security.

One of the primary reasons for concern about the security of federal computer systems is the large amount of personal information held by the federal government. We need assurance from the government that information will be properly maintained, that it will not be used a reason other than for which it was collected. As the Supreme Court stated recently in the Reporter's Committee case "a centralized computer file pose[s] a 'threat to privacy'."⁵⁸ The misuse of personal information contained in government computer systems will have harmful consequences.⁵⁹

⁵⁷ Horning, Neumann, Redell, Goldman & Gordon, "A Review of NCIC 2000" (1989).

⁵⁸ Department of Justice v. Reporters Committee for Freedom of the Press, No. 87-1379, slip. op. at 20 (decided March 22, 1989).

⁵⁹ See generally David Burnham, The Rise of the Computer State (1983), Kenneth C. Laudon, The Dossier Society (1986), David F.

As used in the Act, the term "sensitive" information must be understood to emphasize the importance of protecting the privacy interests of all Americans whose medical, employment, tax, and a host of other records are maintained by the federal government.

I would draw the Committee's attention to an important principle discussed in David Linowes's recent book, Privacy in America.⁶⁰ Mr. Linowes was the chair of the U.S. Privacy Protection Study Commission from 1977 to 1979. His book discusses the problem of the rapid accumulation of personal information in large organizations. He urges organizations to adopt Fair Information Practices, including the requirement of information "minimization" to insure that privacy is protected.⁶¹ According to that principle, only necessary information should be collected.

Now this principle could be at odds with fundamental security practices. For example, audit trails, which enhance system security, may also undercut privacy safeguards. On the one hand an audit trail satisfies an important security goal: it creates a record of all the transactions on a system to determine what changes were made, at what point, and by whom. At the same time, an audit trail generates an activity log of individuals who are using the system: when they worked with the system, and what they

Linowes, Privacy in America (1989), Robert Ellis Smith, Privacy (1980), Alan F. Westin, Privacy and Freedom (1967).

⁶⁰ David F. Linowes, Privacy in America (1989).

⁶¹ Id. at 175. A related principle is that information should only be used for the purpose for which it was collected. Id. at 176.

did. If the system contains an electronic mail capability, then an audit trail might also record the times when messages were sent, the address of the messages, as well as the content.

To the extent that agencies seek to improve system security through the incorporation of audit trails, they will generate an extraordinary amount of transactional information about the activities of people inside and outside of federal government. This information, already in computer form, might then become grist for the mill of employee reviews, censorship, and workplace monitoring.

There is no simple solution to this problem.⁶² Computer security, in the narrow sense, will require audit trails. But privacy protection and the principle of information minimization might argue against excessive use of audit trails. Where will the NSA strike that balance?

A chilling description from Aleksander Solzhenitsyn describes the risk of gathering excessive information:

⁶² A group of CPSR members examined the privacy and security trade-offs of audit trails at a recent meeting. They suggested that the problem might be addressed by: (1) stating clearly the purpose of the audit trail in the system specifications; (2) developing a record destruction procedure for audit trails; (3) limiting the circumstances when an audit trail may be accessed, e.g. when actual data misuse, alteration, or destruction is shown; and (4) isolating audit trails so as to avoid the consolidation of "event" histories. Meeting of Computer Professionals for Social Responsibility, DC Chapter, May 2, 1989. (Summary available from CPSR).

As every person goes through life he fills in a number of forms for the record, each containing a number of questions . . . There are thus hundreds of little threads radiating from every person, millions of threads in all. If these threads were suddenly to become visible, the whole sky would look like a spider's web, and if they materialized like rubber bands, buses and trams and even people would lose the ability to move and the wind would be unable to carry torn-up newspapers or autumn leaves along the streets of the city.⁶³

REMEDIAL OR LEGISLATIVE ACTION

What can be done to get the legislation back on track?

First, the President should rescind NSDD-145. This Decision Directive is responsible for much of the confusion about the roles of the NSA and the NIST. It is doing little to strengthen national security; it may do much to weaken economic competitiveness, restrict scientific inquiry, and undermine open government.

In its place the President should issue a new executive order, revising the federal standard for information classification, and reversing the trend toward secrecy that is threatening our system of open government. As John Shattuck and Muriel Morisey Spence have stated:

⁶³ Quoted in David Burnham, The Rise of the Computer State 47-48 (1983).

The engines of innovation that drive our economy and guarantee our security are powered by open and unfettered communication. Government policy aimed at broadly controlling the communications of information and ideas may soon become irreparably damaging unless it is substantially reversed.⁶⁴

Second, Congress should increase funding for the NIST, contingent on its withdrawal from the M.O.U., so that it has the resources to fulfill the responsibilities it has been assigned under the Act. Without sufficient funding, NIST will continue to go, hat in hand, to the NSA for technical assistance.

Third, this Committee must make clear to the Director of the NSA, the Director of NIST, and the Secretary of Commerce, that the M.O.U. is not in accord with the Computer Security Act, and that, for this reason, neither party can be bound by the agreement. This is a matter of Congressional authority that goes far beyond this specific agreement.

Fourth, the NIST staff responsible for implementing the Act, and those at NSA who are working to assist NIST, must go back to the privacy statutes governing record-keeping practices in the federal agencies. Without a clear understanding of the importance of the Privacy Act and the related statutes, NIST will fail to address a central concern of the Act: the protection of personal privacy.

Fifth, Congress must begin public hearings on the role of encryption technology. For too long data encryption has been left

⁶⁴ "Essay: Needed A Free Flow of Information and Idea," Scientific American, January 1989, at 114.

to the intelligence agencies. Now, it is clear that encryption is the most important technical safeguard for ensuring the privacy and authenticity of all messages that travel along computer networks.⁶⁵

Discussions about government cryptography must become public discussions, regardless of the agencies involved.⁶⁶ We also need to know, in particular and on the record, whether the NSA is engaged in routine monitoring of communications within the United States. And, according to Federal Computer Week, DARPA's Information Science and Technology Office is developing an expert system that can "examine millions of telephone calls a day and discern subtle and complex patterns for follow-up by law enforcement officials."⁶⁷ Has the NSA participated in this work?

Mr. Chairman, fifteen years ago, the Senate Intelligence Committee warned that the NSA's "potential to violate the privacy of Americans is unmatched by any other intelligence agency."⁶⁸

⁶⁵ McLellan, "Internet Computer Network to Use Code to Ensure Privacy," The New York Times, March 21, 1989.

⁶⁶ The NSA has repeatedly tried to restrict the publication of cryptography research. See, e.g., David Burnham, The Rise of the Computer State 139-40 (1983), Kolata, "NSA Asks to Review Papers Before Publication," 215 Science 1485 (March 19, 1982), "Prior Restraints on Cryptography Considered," 208 Science 1442-43 (June 27, 1980).

⁶⁷ Anthes, "DARPA Program to Battle War on Drugs, Terrorism," April 24, 1989, at 1, 53.

⁶⁸ U.S. Senate, Select Committee on Intelligence, Intelligence Activities and the Rights of Americans, Final Report 201 (1976), reprinted in S. Bamford, The Puzzle Palace 473 (1983).

The Chairman of that Committee, Senator Frank Church, said that NSA intelligence-gathering capabilities were essential to the security of the United States. But he also warned that the massive eavesdropping devices and computers of the NSA create a "tremendous potential for abuse."⁶⁹ If ever turned against the communications system of the United States,

no American would have any privacy left . . .
There would be no place to hide.

We must see to it that this agency and all
agencies that possess this technology operate
within the law and under proper supervision,
so that we never cross over that abyss. That
is an abyss from which there is no return.⁷⁰

Mr. Chairman, twelve years ago I was in Washington and had the opportunity to meet with Senator Church after a hearing. I asked him about the role of Congressional oversight in intelligence activities. He left no doubt about its importance. Neither can this Committee.

⁶⁹ National Broadcasting Company, Meet the Press 6 (1975) (NBC television broadcast, August 17, 1975)

⁷⁰ Id.

NATIONAL SECURITY COUNCIL
WASHINGTON, D.C. 20506

F90-876 F90-933
F90-1159 F91-33C

April 1, 1992

Dear Mr. Rotenberg:

This is in further response to your Freedom of Information Act (FOIA) request of September 13, 1990, for "a copy of the revised National Security Decision Directive 145, signed by the President on July 5, 1990." This letter also responds to referrals from the Department of Defense, dated September 28, 1990, and November 20, 1990 (DoD case number 90-FOI-1584/M), of your request to that agency for the same document.

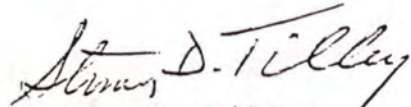
The National Security Council (NSC) staff has completed its review of National Security Directive 42 and determined that a partial text version of the document may be released. The withheld portion of the document is properly classified under the provisions of Executive Order 12356 and, therefore, is exempt from disclosure under 5 U.S.C. 552 (b)(1).

Furthermore, the NSC staff has determined that the release of the format of NSD 42 could cause damage to the national security, and, therefore, the format of this document is properly classified under the provisions of Executive Order 12356. The format of this document is also denied under 5 U.S.C. 552 (b)(1). A redacted copy of the partial text release is enclosed.

You may appeal this denial by writing to the Executive Secretary, National Security Council, Washington, D.C. 20506, within sixty (60) days of the receipt of this letter.

We appreciate your patience while we processed your request.

Sincerely,



Steven D. Tilley
Director
Information Disclosure

Enclosure: a/s

Mr. Marc Rotenberg
Computer Professionals for
Social REsponsibility
1025 Connecticut Avenue, N.W.
Suite 1015
Washington, D.C. 20036

UNCLASSIFIED

July 5, 1990

National Policy for the Security of National
Security Telecommunications and Information
Systems

Continuing advances in microelectronics technology have stimulated an unprecedented growth in the demand for and supply of telecommunications and information processing services within the government and throughout the private sector. As new technologies have been applied, traditional distinctions between telecommunications and information systems have begun to disappear. Although this trend promises greatly improved efficiency and effectiveness, it also poses significant security challenges.

Telecommunications and information processing systems are highly susceptible to interception, unauthorized electronic access, and related forms of technical exploitation, as well as other dimensions of the foreign intelligence threat. The technology to exploit these electronic systems is widespread and is used extensively by foreign nations and can be employed, as well, by terrorist groups and criminal elements. A comprehensive and coordinated approach must be taken to protect the government's national security telecommunications and information systems (national security systems) against current and projected threats. This approach must include mechanisms for formulating policy, overseeing systems security resources programs, and coordinating and executing technical activities.

This Directive establishes initial objectives, policies, and an organizational structure to guide the conduct of activities to secure national security systems from exploitation; establishes a mechanism for policy development and dissemination; and assigns responsibilities for implementation. It is intended to ensure full participation and cooperation among the various existing centers of technical expertise throughout the Executive branch, and to promote a coherent and coordinated defense against the foreign intelligence threat to these systems. This Directive recognizes the special requirements for protection of intelligence sources and methods.

Released
Partial Text of
NSD 42

UNCLASSIFIED

1. Objectives. Ensuring the security of national security systems is vitally important to the operational effectiveness of the national security activities of the government and to military combat readiness. I, therefore, direct that the government's capabilities for securing national security systems against technical exploitation threats be maintained or, if inadequate, improved to provide for:

- a. Reliable and continuing assessment of threats and vulnerabilities, and implementation of appropriate, effective countermeasures;
- b. A technical base within the U.S. Government to achieve this security, and initiatives with the private sector to maintain, complement, or enhance that government technical base and to ensure information systems security products are available to secure national security systems; and,
- c. Effective and efficient application of U.S. Government resources.

2. Policies. In support of these objectives, the following policies are established:

- a. U.S. Government national security systems shall be secured by such means as are necessary to prevent compromise, denial, or exploitation;
- b. Federal agencies shall require that national security systems operated and maintained by U.S. Government contractors likewise be secured.

3. Implementation. This Directive establishes an NSC Policy Coordinating Committee for National Security Telecommunications and Information Systems, an interagency group at the operating level, an executive agent and a national manager to implement these objectives and policies.

4. National Security Council/Policy Coordinating Committee for National Security Telecommunications and Information Systems.

The National Security Council/Policy Coordinating Committee (PCC) for National Security Telecommunications, chaired by the Department of Defense, under the authority of National Security Directives 1 and 10, assumed the responsibility for the National Security Telecommunications NSDD 97 Steering Group. By authority

UNCLASSIFIED

of this Directive, the PCC for National Security Telecommunications is renamed the PCC for National Security Telecommunications and Information Systems, and shall expand its authority to include the responsibilities to protect the government's national security telecommunications and information systems. When addressing issues concerning the security of national security telecommunications and information systems, the membership of the PCC shall be expanded to include representatives of the Secretary of State, the Secretary of the Treasury, the Attorney General, the Secretary of Energy, the Secretary of Commerce, and the Director of Central Intelligence. The National Manager for National Security Telecommunications and Information Systems Security shall be invited as an observer. The Policy Coordinating Committee shall:

- a. Oversee the implementation of this Directive;
- b. Develop policy recommendations and provide guidance to the operating level National Security Telecommunications and Information Systems Security Committee (NSTISSC);
- c. Review and resolve matters referred to it by the NSTISSC in fulfilling the responsibilities outlined in paragraph 5, below;
- d. Be subject to the policies of the Director of Central Intelligence on matters pertaining to the protection of intelligence sources and methods; and,
- e. Recommend for Presidential approval additions or revisions to this Directive as national interests may require.

5. The National Security Telecommunications and Information Systems Security Committee.

- a. The NSTISSC is established to consider technical matters and develop operating policies, procedures, guidelines, instructions, and standards as necessary to implement provisions of this Directive. The Committee shall be chaired by the Assistant Secretary of Defense (Command, Control, Communications and Intelligence) and shall be composed of a voting representative of each of the following:

UNCLASSIFIED

UNCLASSIFIED

The Secretary of State
The Secretary of the Treasury
The Secretary of Defense
The Attorney General
The Secretary of Commerce
The Secretary of Transportation
The Secretary of Energy
Director, Office of Management and Budget
Assistant to the President for National Security
Affairs
Director of Central Intelligence
Chairman of the Joint Chiefs of Staff
Director, Federal Bureau of Investigation
Director, Federal Emergency Management Agency
Administrator, General Services Administration
The Chief of Staff, United States Army
The Chief of Naval Operations
The Chief of Staff, United States Air Force
Commandant, United States Marine Corps
Director, National Security Agency
Manager, National Communications System
Director, Defense Intelligence Agency

b. The NSTISSC shall:

- (1) Develop such specific operating policies, procedures, guidelines, instructions, standards, objectives, and priorities as may be required to implement this Directive;
- (2) Provide systems security guidance for national security systems to Executive departments and agencies;
- (3) Submit annually to the Executive Agent an evaluation of the security status of national security systems with respect to established objectives and priorities;
- (4) Approve the release of cryptologic national security systems technical security material, information, and techniques to foreign governments or international organizations. The concurrence of the Director of Central Intelligence shall be obtained with respect to those activities which he manages;

UNCLASSIFIED

UNCLASSIFIED

(5) Establish and maintain a national system for promulgating the operating policies, instructions, directives, and guidance, which may be issued pursuant to this Directive;

(6) Establish permanent and temporary subcommittees as necessary to discharge its responsibilities;

(7) Make recommendations to the PCC for NSTISSC membership and establish criteria and procedures for permanent observers from other departments or agencies affected by specific matters under deliberation, who may attend meetings upon invitation of the Chairman; and,

(8) Interact, as necessary, with the National Communications System Committee of Principals established by Executive Order 12472 to ensure the coordinated execution of assigned responsibilities.

c. The Committee shall have two subcommittees, one focusing on telecommunications security and one focusing on information systems security. The two subcommittees shall coordinate their actions and recommendations concerning implementation of protective measures, which shall combine and coordinate both areas where appropriate.

d. The Committee shall have a permanent secretariat composed of personnel of the National Security Agency and such other personnel from Executive departments and agencies represented on the Committee as are requested by the Chairman. The National Security Agency shall provide facilities and support as required. Other Executive departments and agencies shall provide facilities and support as requested by the Chairman.

6. The Executive Agent of the Government for National Security Telecommunications and Information Systems Security.

a. Consistent with the authority for communications security given the Secretary of Defense in Executive Order 12333, the Secretary of Defense shall serve as Executive Agent of the Government for National Security Telecommunications and Information Systems Security and shall be responsible for implementing, under his signature, policies and procedures to:

UNCLASSIFIED

(1) Ensure the development, in conjunction with Committee member departments and agencies, of plans and programs to fulfill the objectives of this Directive, including the development of necessary security architectures;

(2) Procure for and provide to Executive departments and agencies and, where appropriate, to government contractors and foreign governments, consistent with the laws of the United States, such technical security material, other technical assistance, and other related services of common concern, as required to accomplish the objectives of this Directive;

(3) Approve and provide minimum security standards and doctrine for systems subject to this Directive; (U)

(4) Conduct, approve, or endorse research and development of techniques and equipment to secure national security systems; and,

(5) Operate, or coordinate the efforts, of U.S. Government technical centers related to national security telecommunications and information systems security.

b. The Executive Agent shall review and assess the National Manager's recommendations on the proposed national security telecommunications and information systems security programs and budgets for the Executive departments and agencies. Where appropriate, alternative systems security recommendations will be provided to agency heads, to National Security Council Committees, and to the OMB. In addition, the Executive Agent shall submit, annually, the security status of national security systems with respect to established objectives and priorities through the National Security Council to the President.

7. The National Manager for National Security Telecommunications and Information Systems Security.

The Director, National Security Agency, is designated the National Manager for National Security Telecommunications and Information Systems Security and is responsible to the Secretary of Defense as Executive Agent for carrying out the foregoing responsibilities. In fulfilling these responsibilities the National Manager shall:

UNCLASSIFIED

- a. Examine U.S. Government national security systems and evaluate their vulnerability to foreign interception and exploitation. Any such activities, including those involving monitoring of official telecommunications, shall be conducted in strict compliance with law, Executive Order and implementing procedures, and applicable Presidential directive. No monitoring shall be performed without advising the heads of the agencies, departments, or services concerned;
- b. Act as the U.S. Government focal point for cryptography, telecommunications systems security, and information systems security for national security systems;
- c. Conduct, approve, or endorse research and development of techniques and equipment to secure national security systems;
- d. Review and approve all standards, techniques, systems, and equipment related to the security of national security systems;
- e. Conduct foreign computer security and communications security liaison, including entering into agreements with foreign governments and with international and private organizations regarding national security systems, except for those foreign intelligence relationships conducted for intelligence purposes by the Director of Central Intelligence. Any such agreements shall be coordinated with affected departments and agencies;
- f. Operate such printing and fabrication facilities as may be required to perform critical functions related to the provisions of cryptographic and other technical security material or services;
- g. Assess the overall security posture of and disseminate information on threats to and vulnerabilities of national security systems;
- h. Operate a central technical center to evaluate and certify the security of national security telecommunications and information systems;

UNCLASSIFIED

- i. Prescribe the minimum standards, methods, and procedures for protecting cryptographic and other technical security material, techniques, and information related to national security systems;
 - j. Review and assess annually the national security telecommunications systems security programs and budgets of Executive departments and agencies of the U.S. Government, and recommend alternatives, where appropriate, for the Executive Agent;
 - k. Review annually the aggregated national security information systems security program and budget recommendations of the Executive departments and agencies of the U.S. Government for the Executive Agent;
 - l. Request from the heads of Executive departments and agencies such information and technical support as may be needed to discharge the responsibilities assigned herein;
 - m. Coordinate with the National Institute for Standards and Technology in accordance with the provisions of the Computer Security Act of 1987 (P.L. 100-235); and
 - n. Enter into agreements for the procurement of technical security material and other equipment, and their provision to Executive departments and agencies, where appropriate, to government contractors, and foreign governments.
8. The Heads of Executive Departments and Agencies shall:
- a. Be responsible for achieving and maintaining secure national security systems within their departments or agencies;
 - b. Ensure that policies, procedures, guidelines, instructions, and standards issued pursuant to this Directive are implemented within their departments or agencies; and
 - c. Provide to the NSTISSC, the Executive Agent, and the National Manager, as appropriate, such information as may be required to discharge responsibilities assigned herein, consistent with relevant law, Executive Order, and Presidential directive.

9. Additional Responsibilities. The Director, Office of Management and Budget, shall:

- a. Specify data to be provided during the annual budget review by Executive departments and agencies on program and budgets relating to security of their national security systems;
- b. Consolidate and provide such data to the National Manager via the Executive Agent; and
- c. Review for consistency with this Directive, and amend as appropriate, OMB policies and regulations which may pertain to the subject matter herein.

10. Nothing in this Directive shall:

- a. Alter or supersede the existing authorities of the Director of Central Intelligence;
- b. Authorize the Committee, the Executive Agent, or the National Manager authority to examine the facilities of other Executive departments and agencies without approval of the head of such department or agency, nor to request or collect information concerning their operation for any purpose not provided for herein;
- c. Amend or contravene the provisions of existing law, Executive Order, or Presidential directive which pertain to the protection of sensitive information, to the protection of national security information, to the privacy aspects or financial management of information systems or to the administrative requirements for safeguarding such resources against fraud, waste, and abuse;
- d. Provide authority to issue policies, procedure, guidelines, instructions, standards, or priorities or operate programs concerning security of systems other than national security systems;
- e. Be intended to establish additional review processes for the procurement of information processing systems;
- f. Alter or rescind policies or programs begun under PD-24 or NSDD-145 that may be pertinent to national security systems. Policies or programs retained pursuant to this provision shall not be construed to apply to systems within the purview of the Computer Security Act of 1987 (PL100-235); or

UNCLASSIFIED



11. For the purposes of this Directive, the following terms shall have the meanings indicated:

a. Telecommunications means the preparation, transmission, communication, or related processing of information (writing, images, sounds or other data) by electrical, electromagnetic, electromechanical, electro-optical, or electronic means;

b. Information Systems means any equipment or interconnected system or subsystems of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data and includes computer software, firmware, and hardware;

c. Telecommunications and Information Systems Security means protection afforded to telecommunications and information systems, in order to prevent exploitation through interception, unauthorized electronic access, or related technical intelligence threats, and to ensure authenticity. Such protection results from the application of security measures (including cryptosecurity, transmission security, emission security, and computer security) to systems which generate, store, process, transfer, or communicate information of use to an adversary, and also includes the physical protection of technical security material and technical security information;

UNCLASSIFIED

d. Technical security material means equipment, components, devices, and associated documentation or other media which pertain to cryptography, or to the securing of telecommunications and information systems;

e. National security systems are those telecommunications and information systems operated by the U.S. Government, its contractors, or agents, that contain classified information or, as set forth in 10 U.S.C. Section 2315, that involves intelligence activities, involves cryptologic activities related to national security, involves command and control of military forces, involves equipment that is an integral part of a weapon or weapon system, or involves equipment that is critical to the direct fulfillment of military or intelligence missions.

12. Except for ongoing telecommunications protection activities mandated by and pursuant to PD-24 and NSDD-145, NSDD-145 is hereby rescinded.



NATIONAL SECURITY AGENCY
CENTRAL SECURITY SERVICE
FORT GEORGE G. MEADE, MARYLAND 20755-6000

Serial: J9104-92
4 March 1993

Computer Professionals for
Social Responsibility
ATTN: Mr. David L. Sobel
666 Pennsylvania Avenue
Suite 303
Washington, DC 20003

Dear Mr. Sobel:

This responds to your Freedom of Information Act (FOIA) request of 11 February 1992 for a copy of NTISSD No. 600. Your request has been processed under the provisions of the FOIA, and the document you request is enclosed.

Sincerely,

Linda I. Miller
LINDA I. MILLER
Chief
Information Policy

Encl:
a/s

NTISSD No. 600
10 April 1990

NTISS

NATIONAL
TELECOMMUNICATIONS
AND
INFORMATION SYSTEMS
SECURITY

COMMUNICATIONS SECURITY

(COMSEC)

MONITORING

~~FOR OFFICIAL USE ONLY~~

NTISS

NATIONAL
TELECOMMUNICATIONS
AND
INFORMATION
SYSTEMS
SECURITY

EXECUTIVE AGENT

10 April 1990

MEMORANDUM FOR THE HEADS OF DEPARTMENTS AND AGENCIES

SUBJECT: Communications Security Monitoring

National Security Decision Directive 145, dated 17 September 1984, assigned to the National Manager for Telecommunications and Automated Information Systems Security the responsibility of examining government telecommunications systems and evaluating their vulnerability to hostile interception and exploitation. The National Manager's examination for such purposes may include the conduct of communications security (COMSEC) monitoring operations.

The accompanying Directive, hereby promulgated, establishes policy and basic procedures and assigns responsibilities for conducting COMSEC monitoring activities. This Directive replaces National COMSEC Instruction No. 4000A, "Guidelines for the Conduct of COMSEC Monitoring Activities," dated 9 February 1984.

Additional copies of the Directive may be obtained from the National Telecommunications and Information Systems Security Committee, Executive Secretariat, National Security Agency.



COMMUNICATIONS SECURITY (COMSEC) MONITORING

INTRODUCTION.	I
PURPOSE AND SCOPE	II
REFERENCES.	III
DEFINITIONS	IV
POLICY.	V
GUIDELINES FOR THE CONDUCT OF COMSEC	
MONITORING.	VI
CONTROL OF MONITORING RECORDS AND	
EQUIPMENT	VII
RESPONSIBILITIES.	VIII

SECTION I - INTRODUCTION

1. The purpose of COMSEC monitoring is to provide unique material, not readily available through other sources, to evaluate the status of U.S. COMSEC. The information collected through COMSEC monitoring is similar to information potentially available to foreign powers through their signals intelligence (SIGINT) collection. Hypothetical projections of the vulnerability of telecommunications, procedures, equipment, and systems, based on technical analysis and modeling, do not always provide comprehensive data for analysis. COMSEC monitoring is, therefore, used to provide the empirical data needed to identify vulnerabilities and afford a basis for correcting them.

SECTION II - PURPOSE AND SCOPE

2. This Directive provides policy and basic procedures for the establishment of COMSEC monitoring programs consistent with law, Executive Orders, and applicable Presidential Directives.¹

3. This Directive is applicable to all U.S. Government departments and agencies engaged in or using the results of COMSEC monitoring. It has been approved by the Attorney General.

¹ References a., b., and c. are pertinent to COMSEC monitoring guidelines and procedures.

4. Technical surveillance countermeasures electronic sweeps, surveillance of non-communications emissions (e.g., radar), and TEMPEST testing are not within the scope of this Directive.

SECTION III - REFERENCES

- a. Communications Act of 1934, Public Law No. 73-416 (as amended).
- b. Omnibus Crime Control and Safe Streets Act of 1968, Public Law No. 90-351 (as amended).
- c. Foreign Intelligence Surveillance Act of 1978, Public Law No. 95-511.
- d. Executive Order 12333, "United States Intelligence Activities," dated 4 December 1981.
- e. National Security Decision Directive Number 145, "National Policy on Telecommunications and Automated Information Systems Security," dated 17 September 1984.

SECTION IV - DEFINITIONS

- 5. COMSEC. Protective measures taken to deny unauthorized persons information derived from telecommunications of the U.S. Government related to national security and to ensure the authenticity of such communications. Such protection results from the application of security measures (including cryptosecurity, transmission security, and emissions security) to telecommunications systems generating, handling, processing, or using classified or sensitive government or government-derived information, the loss of which could adversely affect the national security interest. It also includes the application of physical security measures to COMSEC information or materials.
- 6. COMSEC Monitoring. The act of listening to, copying, or recording transmissions of one's own official telecommunications to provide material for analysis in order to determine the degree of security being provided to those transmissions.
- 7. Contents. When used with respect to a communication, the term includes any information concerning the identity of the parties to such communication or the substance, purport, or meaning of that communication.

8. Electronic Surveillance. The acquisition of the contents of a nonpublic communication by electronic means without the consent of a person who is a party to the communication, but not including the use of radio direction-finding equipment solely to determine the location of a transmitter.

9. Nonpublic Communication. A communication in which the parties thereto have a reasonable expectation of privacy.

10. Telecommunications. The transmission, communication, or processing of information, including the preparation of such information therefore, by electrical, electromagnetic, electro-mechanical, or electro-optical means.

11. Telecommunications Systems. The interconnected devices used to transmit and/or receive communications or process telecommunications; the devices may be electrical, electromagnetic, electromechanical, or electro-optical.

12. Government Telecommunications. Telecommunications of any employee, officer, contractor, or other entity of the U.S. Government which concern an official purpose of government and which are transmitted over a telecommunications system owned or leased by the U.S. Government or a government contractor. (See Telecommunications and Telecommunications Systems, above.)

SECTION V - POLICY

13. U.S. Government departments and agencies will conduct COMSEC monitoring activities only as necessary to determine the degree of security provided to government telecommunications and aid in countering their vulnerability. Such activities shall be conducted in strict compliance with law, Executive Orders, applicable Presidential Directives, and this Directive.

14. Government telecommunications systems are subject to COMSEC monitoring by duly authorized government entities.² Users of these systems must be properly notified in advance, in accordance with the guidelines in paragraph 24 below, that their use of these systems constitutes consent to monitoring for

² Individual department or agency regulations shall specify which internal organization(s) of that department or agency are authorized to conduct COMSEC monitoring operations.

COMSEC purposes. The use of such systems by any person shall constitute implied consent to the monitoring for COMSEC purposes of communications carried over them.³ The government shall not monitor telecommunications systems which are owned or leased by government contractors for their own use without first obtaining the express written approval of the chief executive officer of the contractor organization (or his/her designee) and the written opinion of the general counsel of the department or agency which is actually performing the monitoring that procedures, such as those contained in paragraph 24 below, have been implemented sufficiently to afford notice to the contractor organization's employees.

15. The government shall not monitor for COMSEC purposes the contents of any telecommunications when such monitoring would constitute electronic surveillance.

16. In accordance with procedures approved by the Attorney General, information acquired incidentally from government telecommunications during the course of authorized COMSEC monitoring which relates directly to a significant crime will be referred to the military commander or law enforcement agency having appropriate jurisdiction. When taking such action, the general counsel of the department or agency which is actually performing the COMSEC monitoring shall be notified promptly. The results of COMSEC monitoring may not be used in a criminal prosecution without prior consultation with the general counsel of the department or agency which actually performed the monitoring.

17. The results of COMSEC monitoring shall not be used to produce foreign intelligence or counterintelligence, as defined in Reference d. However, the results of COMSEC monitoring of U.S. and Allied military exercise communications may be used for exercise intelligence purposes under procedures prescribed in applicable directives.

18. No department or agency may monitor the telecommunications of another department or agency for COMSEC purposes without the express prior written approval of the head (or his/her designee) of the department or agency to be monitored, except as provided for the subparagraph 32.b.

³ Consent to COMSEC monitoring is required of only one party to a conversation or transmission. See References a. (particularly 47 U.S.C. § 605), b. (particularly 18 U.S.C. § 2511), and c. (particularly 50 U.S.C. § 1801).

19. COMSEC monitoring shall be conducted in strict accordance with operational procedures which minimize the possibility that unnecessary communications content will be acquired. Such procedures shall be consistent with the guidelines contained herein and shall be approved in writing by the general counsel of the department or agency issuing the procedures.

SECTION VI - GUIDELINES FOR THE CONDUCT OF COMSEC MONITORING

20. COMSEC monitoring may be undertaken for the following reasons appropriate to the purpose described in paragraph 1., above:

a. To collect operational signals needed to measure the degree of security being achieved by U.S. codes, cryptographic equipment and devices, COMSEC techniques, and related materials.

b. To provide a basis from which to assess the types and value of information subject to loss through intercept and exploitation of government telecommunications.

c. To provide an empirical basis for improving the security of government telecommunications against SIGINT exploitation.

d. To assist in determining the effectiveness of electronic countermeasures/electronic counter-countermeasures (ECM/ECCM), cover and deception actions, and operations security (OPSEC) measures.

e. To identify government telecommunications signals that exhibit unique external signal parameters, signal structures, modulation schemes, radio fingerprints, etc., that could provide SIGINT elements of foreign powers the capability to identify specific targets for subsequent geopositioning and exploitation purposes.

f. To provide empirical data to train users of government telecommunications systems in proper COMSEC techniques and measures.

g. To evaluate the effectiveness of COMSEC education and training programs.

h. To train personnel and to test the capability of COMSEC monitoring equipment.

i. To determine OPSEC indications that can be obtained from telecommunications in support of OPSEC surveys.

21. The following categories of telecommunications are considered public for purposes of this Directive. Accordingly, acquisition of the contents of any communications in these categories which may occur in the course of locating or examining government telecommunications is not electronic surveillance.

a. Radio or television broadcast communications, whether commercial, public or educational, intended for the information or entertainment of the general public.

b. Public safety, citizens band, amateur radio, and similar radio systems licensed by the government for public use or access.

c. Any communications in portions of the electromagnetic spectrum which are allocated by the government for its own use.

22. No incidentally acquired nonpublic communication, as defined above, may be monitored beyond the point where a determination can reasonably be made that it is nonpublic. A record of the acquisition may be kept for signal identification and avoidance purposes; such a record may describe the signal parameters (frequency, modulation, type, and timing) but may not identify the parties or the meaning of the communication.

23. Contents of any nonpublic communication may not be deliberately acquired as part of a procedure for locating, identifying, or monitoring a government communication.

24. Notice of existence of COMSEC monitoring, in conformance with paragraph 14 above, can be accomplished by any of the following means or any combination thereof which the legal counsel of the affected department or agency considers legally sufficient to achieve proper notification in terms of content, prominence, and specificity:

- a. Decals placed on the transmitting or receiving devices.
- b. A notice in the daily bulletin or similar medium.
- c. A specific memorandum to users.
- d. A statement on the cover of the official telephone book or communications directory.
- e. A statement in the standing operating procedures, communications-electronics operating instructions, or similar documents.

SECTION VII - CONTROL OF MONITORING RECORDS AND EQUIPMENT

25. All reports, logs, and material produced in the course of COMSEC monitoring will be afforded protection commensurate with the classification of the information and the sensitivity of the monitored activity. Reports or material produced from COMSEC monitoring which identify security weaknesses of the monitored activity will be classified at least CONFIDENTIAL and downgraded to UNCLASSIFIED when security weaknesses are corrected.

26. Interim and final reports may be disseminated only to the extent necessary for COMSEC purposes except as provided for in paragraph 16 above. These reports shall not contain any information extraneous to COMSEC purposes or names of individuals or sufficient data to identify the source except in an official capacity; e.g., "the radio operator on watch." Dissemination controls should be expressly stated on each report.

27. All COMSEC monitoring recordings and written records, logs, and notes shall be destroyed as soon as operationally feasible, except as provided for in paragraph 16 above.

28. Information extraneous to COMSEC purposes will not be recorded, reported, noted, logged, or filed, except as provided for in paragraph 16. If within the capabilities of COMSEC monitoring equipment, any such information that is inadvertently acquired shall be expunged upon recognition. All monitoring records shall be reviewed for identification and expungement of extraneous information within a reasonable time after they are created.

29. Access to, and dissemination of, COMSEC monitoring recordings or written records, reports, logs, and notes shall be limited to that which is necessary for COMSEC purposes. No access to, or dissemination of, such materials beyond COMSEC operational elements shall be allowed until such material is reviewed to determine that it contains no information extraneous to COMSEC purposes.

30. COMSEC monitoring equipment shall be safeguarded to prevent unauthorized access and use.

SECTION VIII - RESPONSIBILITIES

31. Heads of departments and agencies shall:

a. Provide for and conduct COMSEC monitoring operations as they deem appropriate, subject to the provisions of law, Executive Orders, applicable Presidential Directives, and this Directive.

b. Develop procedures for the conduct of COMSEC monitoring, consistent with the policy and procedures herein. Such procedures shall be approved by the Attorney General.

c. Establish procedures to notify, as specified in paragraph 24, all personnel and contractors who are present on facilities of the department or agency of the policy in paragraph 14 above.

d. Certify biennially to the National Manager for Telecommunications and Automated Information Systems Security those organizations whose personnel and contractors have been notified of the provisions of this Directive after determination by the department or agency general counsel or legal counsel that notification is legally sufficient to ensure implied consent.

32. The National Manager for Telecommunications and Automated Information Systems Security shall:

a. Advise and assist other departments and agencies in establishing their operating procedures to implement this Directive.

b. Conduct COMSEC monitoring of government telecommunications as necessary to discharge his responsibilities under Reference e., in accordance with the following guidelines:

(1) Monitor fielded government cryptography, except encrypted telephone communications, following written notice to the head (or his/her designee) of the organization whose encrypted telecommunications are to be monitored. If there is a substantial likelihood that monitoring of encrypted telecommunications will result in the acquisition of plaintext communications, other than short-duration plaintext operator conversations associated with establishing a secure condition, the guidelines of subparagraph 32.b.(2), below, shall be followed. Monitoring of encrypted telephone communications may be carried out in accordance with the requirements of paragraph 14.

(2) Monitor plaintext government telecommunications, following case-by-case notice to the head (or his/her designee) of the department or agency whose telecommunications are to be monitored. Such notice shall include a detailed plan for the conduct of the monitoring, a detailed description of the reasons for the monitoring (in accordance with paragraph 20 above), the reasons why less intrusive means of evaluating telecommunications systems vulnerabilities are inadequate, and the expected results of the monitoring. Monitoring shall not begin until the department or agency to be monitored has been afforded a thirty day period of time to make any objections known to the National Manager. Objections must be specific and must provide facts sufficient to allow independent review of the basis of that objection. No monitoring shall begin until such time as those objections are resolved. If possible, such objections shall be resolved in negotiations between the National Manager and the head of the department or agency to be monitored. If resolution cannot be reached at that level, the National Manager may refer the matter to the Attorney General, if the remaining objection is on legal grounds, or the Executive Agent of the Government for Telecommunications and Information Systems Security, if the remaining objection is on other than legal grounds. Except as provided for in paragraph 16 above, the results of COMSEC monitoring of plaintext communications shall not be disseminated to departments or agencies other than those affected without the prior approval of the head (or his/her designee) of such department or agency.

(3) Authorize and conduct emergency COMSEC monitoring of specific public telecommunications of the government (excluding government contractor telecommunications) prior to the receipt of certification as required by subparagraph 31.d., when a delay in initiating COMSEC monitoring may have a serious impact upon U.S. national security interests or a threat to human life is imminent. Such emergency COMSEC monitoring shall not exceed a period of 72 hours, and shall be conducted only upon:

(a) Request by the head of a U.S. Government department, agency, or military service (or his/her designee) for monitoring of its own telecommunications, and

(b) Personal determination of the National Manager that the necessity for COMSEC monitoring exists, and prompt notification to the Attorney General and the head of the requesting organization (or his/her designee) that such monitoring has been initiated, and

(c) Determination that there is insufficient time to satisfy the requirement of subparagraph 31.d., above.

DISTRIBUTION:

NSA
NSC
OMB (Intel Branch NSD)
OASD (C3I/IS) (2)
ODUSD(P) SP&P
DODSI
DA (SAIS-ADS) (15)
CMC (CC) (5)
The Joint Staff (J6K) (2)
The Joint Staff (DIRM/SCD/ISOB)
CDRUSELNORAD (2)
USCINCLANT (J6) (2)
USCINCCENT (CCJ6) (4)
USCINCEUR (ECJ6) (2)
USCINCFOR (FCJ6) (2)
USCINCPAC (J6) (2)
USCINCSO (SCJ6) (2)
USCINCSpace (J4-J6) (2)
USCINCSOC (SOJ6) (2)
CINCSAC (SC) (2)
USCINCTrans (TCJ6) (2)
HQ AFCC/DSS (2)
HQ USAF (SCTX) (3)
AFCSC (SRMP) (10)
AFCSC/SRVT
COMUSFORCARIB (J6) (2)
COMUSFJAPAN (J6) (2)
COMUSFKOREA (J6) (2)
Defense Courier Service (2)
DIA (DSE-2B) (10)
DIS (V0410) (5)
DIS (V0060)
DLA (DLA-IA) (2)
DNA (LECD)
CDR JTC3A
COMNAVSECGRU (G-34) (4)
COMDT COGARD (G-TTS-4) (3)
COMCOGARDLANTAREA
COMCOGARDPACAREA
COMCOGARDONE
COMCOGARDTWO
COMCOGARDFIVE
COMCOGARDSEVEN
COMCOGARDEIGHT
COMCOGARDNINE
COMCOGARDELEVEN

COMCOGARDMLCLANT
COMCOGARDMLCPAC
COMCOGARDTHIRTEEN
COMCOGARDFOURTEEN
COMCOGARDSEVENTEEN
COMSPAWARSSYSCOM (PMW 151-21) (3)
DCMS (T60) (6)
CG MCDEC (DEVGEN C3) (2)
DCMS (T2) (2)
Dept. of Agriculture (MSD/FAS) (2)
Dept. of Commerce (NTIA) (2)
Dept. of Energy (CSTM) (2)
Dept. of Health & Human Services (IG) (2)
Dept. of Interior (AMO) (2)
Dept. of Justice (JMD/SEPS) (2)
Dept. of State (IM/SO/TO/INFS/NCS) (4)
Dept. of Transportation (OIS M-70) (2)
Dept. of Treasury (MST) (10)
CIA (OC-CSD) (2)
CIA (DIR OIT) (2)
CIA (ISSG/OS) (2)
CIA (Chief, TEMPEST Division, (OS) (2)
CIA (Chief INFOSEC OIT)
DIR, IC STAFF (IIHC) (2)
DIR, IC STAFF (CCISCMO) (2)
DIR, IC STAFF (Policy and Planning Staff) (2)
DCA (Code DIP) (5)
DMA (TSC)
DMA (IS)
Drug Enforcement Administration (AIOC) (2)
FAA (ADL-15) (6)
FBI (TSD) (5)
FCC (OMD) (2)
FEMA (NP-IR) (7)
GSA (KVI) (6)
NASA (NIS)
NASA (TS) (2)
NASA (NT)
NCS (MGR) (2)
NRC (5721-NMBB) (2)
USDELMC
WHCA

ISSUES

IN SCIENCE AND TECHNOLOGY

National Academy of Sciences
National Academy of Engineering
Institute of Medicine

FORUM

Keeping fewer secrets

Kudos to Steven Aftergood for his article. His central goal—"that the present Cold War classification system should be scrapped and replaced by an information policy that is founded on genuine national security requirements"—should be endorsed by every scientific organization in the United States. The current system imposes significant costs on scientific innovation; it also limits government accountability, as our experience in trying to document the development of the Digital Signature Standard (DSS) makes clear.

The DSS is a standard that is important for the future of computer network communications and is also closely tied to developments in cryptography and communications security. It is fundamentally intended to serve the civilian and commercial communities. Computer Professionals for Social Responsibility (CPSR) is currently litigating a Freedom of Information Act case in order to determine the

role of the National Security Agency (NSA) in its development. We were interested to learn whether the NSA was adhering to the requirements of the Computer Security Act of 1987, which was intended to get the intelligence community out of the business of setting technical standards in the computer field. It was passed in response to NSDD-145, President Reagan's classified directive on computer security, which many agreed unnecessarily restricted the open exchange of information.

We have learned that the proposed DSS was developed by the NSA and that the patent is held by an NSA employee. We have also learned that the vast majority of records we requested from the National Institute of Standards and Technology, the agency with the legal authority to develop the DSS, are in the possession of the NSA. This "shell game" permits the NSA to restrict access to documents.

One correction to the article: Aftergood writes that "until May of this year not a single Bush ad-

ministration NSD had ever been made public." In fact, on April 1, 1992, NSD-42 (the new version of NSDD-145) was released to CPSR after we initiated litigation to compel its disclosure. To our knowledge, this was the first Bush NSD released to the public. Not surprisingly, the revised directive indicated that the White House seeks to transfer authority for computer security from the civilian sector back to the intelligence community.

Therein lies the problem: Secret policies promote secret government and permit the abuse of power.

MARC ROTENBERG
Director
Computer Professionals for Social
Responsibility
Washington, D.C.

CPSR

August 11, 1992

Representative Jack Brooks
Chairman
House Judiciary Committee
2138 Rayburn House Office Bldg.
Washington, DC 20515-6216

Dear Mr. Chairman:

Earlier this year, you held hearings before the Subcommittee on Economic and Commercial Law on the threat of foreign economic espionage to U.S. corporations. Among the issues raised during the hearings were the future of computer security authority and the efforts of government agencies to restrict the use of new technologies, such as cryptography.

As a national organization of computer professionals interested in the policies surrounding civil liberties and privacy, including computer security and cryptography, CPSR supports your efforts to encourage public dialogue of these matters. Particularly as the United States becomes more dependent on advanced network technologies, such as cellular communications, the long-term impact of proposed restrictions on privacy-enhancing techniques should be carefully explored in a public forum.

When we had the opportunity to testify before the Subcommittee on Legislation and National Security in May, 1989 on the enforcement of the Computer Security Act of 1987, we raised a number of these issues. We write to you now to provide new information about the role of the National Security Agency in the development of the Digital Signature Standard and the recent National Security Directive on computer security authority. The information that we have gathered suggests that further hearings are necessary to assess the activities of the National Security Agency since passage of the Computer Security Act of 1987. (Several of the documents described here are reproduced in the CPSR Cryptography and Privacy Sourcebook which accompanies this letter.)

CPSR Washington Office
666 Pennsylvania Ave. S.E.
Suite 303
Washington, DC 20003
202 544-9240
Fax 202 547-5481/2
rotenberg@washofc.cpsr.org

Marc Rotenberg, Director
Richard Cville, Program Director
David Sobel, Staff Counsel

CPSR National Office
P.O. Box 717
Palo Alto, CA 94302
415 322-3778
Fax 415 322-3798
Nikki Draper, Office Manager
cpsr@csli.stanford.edu

CPSR Cambridge Office
P.O. Box 962
Cambridge, MA 02142
617 864-7329
Gary Chapman, Director
chapman@satfron.lcs.mit.edu

Advisory Board
Herbert L. Abrams
John Backus
Paul Brest
David Burnham
Dorothy Denning
Carol Edwards
Douglas Engelbart
Admiral Noel Gayler
Adele Goldberg
Richard Karp
Barbara Liskov
Elliot Maxwell
James Martin
Eli Noam
Karen Nussbaum
Severo M. Ornstein
Anthony Ralston
John Shattuck
Herbert Simon
Robert E. Tarjan
Robert W. Taylor
Lawrence Tesler
Sherry Turkle

Board of Directors

President
Eric Roberts

Chairperson
Jeff Johnson

Secretary
Todd Newman

Treasurer
Rodney Hoffman

Directors
Cathy Cook
Paul Hyland
Lesley Kalmin
Patti Lowe
Ivan Milman
Ronni Rosenberg
Douglas Schuler
Dan Williams
Terry Winograd
Coralee Whitcomb

The National Security Agency
and the Digital Signature Standard

Through the Freedom of Information Act, CPSR has recently learned that the NSA was the driving force behind the selection and development of the Digital Signature Standard (DSS). We believe that the NSA's actions contravene the Computer Security Act of 1987. We have also determined that the National Institute of Standards and Technology (NIST) attempted to shield the NSA's role in the development of the DSS from public scrutiny.

The Digital Signature Standard will be used for the authentication of computer messages that travel across the public computer network. Its development was closely watched in the computer science community. Questions about the factors leading to the selection of the standard were raised by a Federal Register notice, 56 Fed. Reg. 42, (Aug 30, 1991), in which NIST indicated that it had considered the impact of the proposed standard on "national security and law enforcement," though there was no apparent reason why these factors might be considered in the development of a technical standard for communications security.

In August 1991, CPSR filed a FOIA request with the National Institute of Standards and Technology seeking all documentation relating to the development of the DSS. NIST denied our request in its entirety. The agency did not indicate that they had responsive documents from the National Security Agency in their files, as they were required to do under their own regulations. 15 C.F.R. § 4.6(a)(4) (1992). In October 1991, we filed a similar request for documents concerning the development of the DSS with the Department of Defense. The Department replied that they were forwarding the request to the NSA, from whom we never received even an acknowledgement of our request.

In April 1992, CPSR filed suit against NIST to force disclosure of the documents. CPSR v. NIST, et al., Civil Action No. 92-0972-RCL (D.D.C.). As a result of that lawsuit, NIST released 140 out of a total of 142 pages. Among those documents is a memo from Roy Saltman to Lynn McNulty which suggests that there were better algorithms available than the one NIST eventually recommended for adoption. If that is so, why did NIST recommend a standard that its own expert believed was inferior?

Further, NIST was required under Section 2 of the Computer Security Act to develop standards and guidelines to "assure the cost-effective security and privacy of sensitive information in federal systems." However, the algorithm

selected by NIST as the DSS was purposely designed to minimize privacy protection: its use is limited to message authentication. Other algorithms that were considered by NIST included both the ability to authenticate messages and the capability to incorporate privacy-enhancing features. Was NSA's interest in communication surveillance one of the factors that lead to the NIST decision to select an algorithm that was useful for authentication, but not for communications privacy?

Most significantly, NIST also disclosed that 1,138 pages on the DSS that were created by the NSA were in their files and were being sent back to the NSA for processing. Note that only 142 pages of material were identified as originating with NIST. In addition, it appears that the patent for the DSS is filed in the name of an NSA contractor.

The events surrounding the development of the Digital Signature Standard warrant further Congressional investigation. When Congress passed the Computer Security Act, it sought to return authority for technical standard-setting to the civilian sector. It explicitly rejected the proposition that NSA should have authority for developing technical guidelines:

Since work on technical standards represents virtually all of the research effort being done today, NSA would take over virtually the entire computer standards job from the [National Institute of Standards and Technology]. By putting the NSA in charge of developing technical security guidelines (software, hardware, communications), [NIST] would be left with the responsibility for only administrative and physical security measures -- which have generally been done years ago. [NIST], in effect, would on the surface be given the responsibility for the computer standards program with little to say about the most important part of the program -- the technical guidelines developed by NSA.

Government Operation Committee Report at 25-26, reprinted in 1988 U.S. Code Cong. and Admin. News at 3177-78. See also Science Committee Report at 27, reprinted in 1988 U.S.C.A.N. 3142.

Despite the clear mandate of the Computer Security Act, NSA does, indeed, appear to have assumed the lead role in the development of the DSS. In a letter to MacWeek magazine last fall, NSA's Chief of Information Policy acknowledged that the Agency "evaluated and provided candidate algorithms including the one ultimately selected by NIST." Letter from Michael S. Conn to Mitch Ratcliffe, Oct. 31, 1991. By its own

admission, NSA not only urged the adoption of the DSS -- it actually "provided" the standard to NIST.

The development of the DSS is the first real test of the effectiveness of the Computer Security Act. If, as appears to be the case, NSA was able to develop the standard without regard to recommendations of NIST, then the intent of the Act has clearly been undermined.

Congress' intent that the standard-setting process be open to public scrutiny has also been frustrated. Given the role of NSA in developing the DSS, and NIST's refusal to open the process to meaningful public scrutiny, the public's ability to monitor the effectiveness of the Computer Security Act has been called into question.

On a related point, we should note that the National Security Agency also exercised its influence in the development of an important standard for the digital cellular standards committee. NSA's influence was clear in two areas. First, the NSA ensured that the privacy features of the proposed standard would be kept secret. This effectively prevents public review of the standard and is contrary to principles of scientific research. The NSA was also responsible for promoting the development of a standard that is less robust than other standards that might have been selected. This is particularly problematic as our country becomes increasingly dependent on cellular telephone services for routine business and personal communication.

Considering the recent experience with the DSS and the digital cellular standard, we can anticipate that future NSA involvement in the technical standards field will produce two results: (1) diminished privacy protection for users of new communications technologies, and (2) restrictions on public access to information about the selection of technical standards. The first result will have severe consequences for the security of our advanced communications infrastructure. The second result will restrict our ability to recognize this problem.

However, these problems were anticipated when Congress first considered the possible impact of President Reagan's National Security Decision Directive on computer security authority, and chose to develop legislation to promote privacy and security and to reverse efforts to limit public accountability.

National Security Directive 42

Congressional enactment of the Computer Security Act was a response to President Reagan's issuance of National

Security Decision Directive ("NSDD") 145 in September 1984. It was intended to reverse an executive policy that enlarged classification authority and permitted the intelligence community broad say over the development of technical security standards for unclassified government and non-government computer systems and networks. As noted in the committee report, the original NSDD 145 gave the intelligence community new authority to set technical standards in the private sector:

[u]nder this directive, the Department of Defense (DOD) was given broad new powers to issue policies and standards for the safeguarding of not only classified information, but also other information in the civilian agencies and private sector which DOD believed should be protected. The National Security Agency (NSA), whose primary mission is one of monitoring foreign communications, was given the responsibility of managing this program on a day-to-day basis.

H. Rep. No. 153 (Part 2), 100th Cong., 1st Sess. 6 (1987). The legislation was specifically intended to override the Presidential directive and to "greatly restrict these types of activities by the military intelligence agencies ... while at the same time providing a statutory mandate for a strong security program headed up by [NIST], a civilian agency." Id. at 7.

President Bush issued National Security Directive ("NSD") 42 on July 5, 1990. On July 10, 1990, Assistant Secretary of Defense Duane P. Andrews testified before the House Subcommittee on Transportation, Aviation, and Materials on the contents of the revised NSD. The Assistant Secretary stated that the "the new policy is fully compliant with the Computer Security Act of 1987 (and the Warner Amendment) and clearly delineates the responsibilities within the Federal Government for national security systems."

On August 27, 1990, CPSR wrote to the Directorate for Freedom of Information of the Department of Defense and requested a copy of the revised NSD, which had been described by an administration official at the July hearing but had not actually been disclosed to the public. CPSR subsequently sent a request to the National Security Council seeking the same document. When both agencies failed to reply in a timely fashion, CPSR filed suit seeking disclosure of the Directive. CPSR v. NSC, et al., Civil Action No. 91-0013-TPJ (D.D.C.).

The Directive, which purports to rescind NSDD 145, was recently disclosed as a result of this litigation CPSR initiated against the National Security Council.

The text of the Directive raises several questions concerning the Administration's compliance with the Computer Security Act:

1. The new NSD 42 grants NSA broad authority over "national security systems." This phrase is not defined in the Computer Security Act and raises questions given the expansive interpretation of "national security" historically employed by the military and intelligence agencies and the broad scope that such a term might have when applied to computer systems within the federal government.

If national security now includes international economic activity, as several witnesses at your hearings suggested, does NSD 42 now grant NSA computer security authority in the economic realm? Such a result would clearly contravene congressional intent and eviscerate the distinction between civilian and "national security" computer systems.

More critically, the term "national security systems" is used throughout the document to provide the Director of the National Security Agency with broad new authority to set technical standards. Section 7 of NSD 42 states that the Director of the NSA, as "National Manager for National Security Telecommunications and Information Systems Security," shall

* * *

c. Conduct, approve, or endorse research and development of techniques and equipment to secure national security systems.

d. Review and approve all standards, techniques, systems, and equipment, related to the security of national security systems.

* * *

h. Operate a central technical center to evaluate and certify the security of national security telecommunications and information systems.

(Emphasis added)

Given the recent concern about the role of the National Security Agency in the development of the Digital Signature Standard, it is our belief that any standard-setting authority created by NSD 42 should require the most careful public review.

2. NSD 42 appears to grant the NSA new authority for information security. This is a new area for the agency; NSA's role has historically been limited to communications security. Section 4 of the directive provides as follows:

The National Security Council/Policy Coordinating Committee (PCC) for National Security Telecommunications, chaired by the Department of Defense, under the authority of National Security Directives 1 and 10, assumed the responsibility for the National Security Telecommunications NSDD 97 Steering Group. By authority of this directive, the PCC for National Security Telecommunications is renamed the PCC for National Security Telecommunications and Information Systems, and shall expand its authority to include the responsibilities to protect the government's national security telecommunications and information systems.

(Emphasis added).

Thus, by its own terms, NSD 42 "expands" DOD's authority to include "information systems." What is the significance of this new authority? Will it result in military control of systems previously deemed to be civilian?

3. NSD 42 appears to consolidate NSTISSC (The National Security Telecommunications and Information Systems Security Committee) authority for both computer security policy and computer security budget determinations.

According to section 7 of the revised directive, the National Manager for NSTISSC shall:

j. Review and assess annually the national security telecommunications systems security programs and budgets of Executive department and agencies of the U.S. Government, and recommend alternatives, where appropriate, for the Executive Agent.

NTISSC has never been given budget review authority for federal agencies. This is a power, in the executive branch, that properly resides in the Office of Management and Budget. There is an additional concern that Congress's ability to monitor the activities of federal agencies may be significantly curtailed if this NTISSC, an entity created by presidential directive, is permitted to review agency budgets in the name of national security.

4. NSD 42 appears to weaken the oversight mechanism established by the Computer Security Act. Under the Act, a Computer Systems Security and Privacy Advisory Board was

established to identify emerging issues, to inform the Secretary of Commerce, and to report findings to the Congressional Oversight Committees. § 3, 15 U.S.C. § 278g-4(b).

However, according to NSD 42 NSTISSC is established "to consider technical matters and develop operating policies, procedures, guidelines, instructions, and standards as necessary to implement provisions of this Directive." What is the impact of NSTISSC authority under NSD 42 on the review authority of the Computer Systems Security and Privacy Advisory Board created by the Computer Security Act?

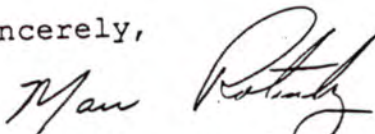
Conclusion

Five years after passage of the Computer Security Act, questions remain about the extent of military involvement in civilian and private sector computer security. The acknowledged role of the National Security Agency in the development of the proposed Digital Signature Standard appears to violate the congressional intent that NIST, and not NSA, be responsible for developing security standards for civilian agencies. The DSS experience suggests that one of the costs of permitting technical-standard setting by the Department of Defense is a reduction in communications privacy for the public. The recently released NSD 42 appears to expand DOD's security authority in direct contravention of the intent of the Computer Security Act, again raising questions as to the role of the military in the nation's communications network.

There are also questions that should be pursued regarding the National Security Agency's compliance with the Freedom of Information Act. Given the NSA's increasing presence in the civilian computing world, it is simply unacceptable that it should continue to hide its activities behind a veil of secrecy. As an agency of the federal government, the NSA remains accountable to the public for its activities.

We commend you for opening a public discussion of these important issues and look forward to additional hearings that might address the questions we have raised.

Sincerely,



Marc Rotenberg, Director
CPSR Washington Office

Enclosures

Governmental Restrictions on the Development and Dissemination of Cryptographic Technologies: The Controversy Over the Digital Signature Standard

by

David L. Sobel, Esq.

David L. Sobel, Legal Counsel of Computer Professionals for Social Responsibility, discusses the impact of national security interests, and the involvement of the National Security Agency in the development of digital signature standards (DSS) by the National Institute of Standards and Technology. DSS enables correspondents to authenticate the integrity of electronically transmitted data in governmental and commercial transactions.

Mr. Sobel argues that the NSA's propensity for secrecy and its desire to retard the development of technologies, which would interfere with its ability to intercept telecommunications traffic, has resulted in a level of NSA involvement in the development of DSS that is contrary to Congress' intentions in enacting the Computer Security Act of 1987. Mr. Sobel further argues that misplaced national security concerns have compromised U.S. competitiveness in the development of encryption technology for commercial purposes.

This article is adapted from a paper presented by Mr. Sobel at the Twentieth Annual Telecommunications Policy Research Conference in Solomons Island, Maryland on September 12-14, 1992.

On August 30, 1991, the National Institute of Standards and Technology ("NIST") published a notice in the Federal Register proposing a federal digital signature standard ("DSS"). The NIST proposal, and details of the standard setting process that recently have come to light, raise substantial questions concerning the future of U.S. information policy in general and cryptographic technology in particular.

The Impact of Government Encryption Standards

The DSS provides a means of authenticating the integrity of electronically transmitted data and the identity of the sender. According to NIST, the standard is "applicable to all federal departments and agencies for the protection of unclassified information," and is "intended for use in electronic mail, electronic funds transfer, electronic data

interchange, software distribution, data storage, and other applications which require data integrity assurance and data origin authentication."¹

With governmental and commercial transactions increasingly dependent upon the reliability and integrity of such telecommunications applications, authentication techniques are indispensable. As NIST's Associate Director for Computer Security, Lynn McNulty, has said, digital signature technology "will be an important part of re-engineering the business practices that we've used for so many years in government and other parts of society The signature will be absolutely critical in certain areas where, because of statute or practice, we currently require a written signature on paper."²

While use of the proposed DSS would be mandatory only for federal agencies, its adoption

by the government would have a substantial impact on the private sector. Vendors will need to offer products for the government that meet the federal standard and are thus likely to design all of their products to conform to its requirements.³ Thus, the Data Encryption Standard ("DES"), which was adopted by NIST's predecessor, the National Bureau of Standards, as a government standard in 1977, was quickly adopted by the American National Standards Institute and became the worldwide industry standard.

"National Security" Interests

In its Federal Register notice, NIST stated that it had selected the DSS after evaluating several alternatives and that the agency had "followed the mandate contained in section 2 of the Computer Security Act of 1987 that NIST develop standards and guidelines to ' . . . assure the cost-effective security and privacy of sensitive information in Federal systems.'"⁴

The reference to the Computer Security Act was significant because, in enacting the statute, Congress sought to vest civilian computer security authority in NIST and to limit the role of the National Security Agency ("NSA").⁵ When Congress enacted the legislation, it expressed particular concern that NSA, a military intelligence agency, would improperly limit public access to information in a manner incompatible with civilian standard setting.⁶ The House Report notes that NSA's

natural tendency to restrict and even deny access to information that it deems important would disqualify that agency from being put in charge of the protection of non-national security information in the view of many officials in the civilian agencies and the private sector.

NSA's reputation for secrecy is well-known and well-deserved. In the years following the Second World War, the making and breaking of secret codes became increasingly important to the U.S. national security establishment.⁷ The National Security Agency, based at Fort George G. Meade, Maryland, was created by order of President Truman in 1952 and tasked with primary responsibility for communications intelligence (COMINT)—intercepting and deciphering the

secret communications of foreign governments. By some accounts, NSA is capable of acquiring and automatically scanning most, if not all, of the electronic messages that enter, leave or transit the United States.⁸ The agency itself refuses to confirm or deny published information concerning its capabilities.

In the 40 years since its creation, NSA has enjoyed a virtual monopoly in the area of cryptographic technology within the United States. Believing its mission requires that such technology be closely held, the agency has actively sought to maintain its monopoly and to suppress the private, non-governmental development and dissemination of cryptography. The motivation behind NSA's efforts to suppress cryptographic know-how is obvious—as the ability to securely encrypt information becomes more widespread, the agency's collection work becomes more difficult and time-consuming.

NSA's efforts to maintain its monopoly have extended into the area of export and trade policy. The export of software products containing cryptographic features is governed by the International Traffic in Arms Regulations ("ITAR"), administered by the Office of Defense Trade Controls at the Department of State.⁹ In addition to software products specifically designed for military purposes, the ITAR "Munitions List" includes a wide range of commercial software containing encryption capabilities.¹⁰ Under the export licensing scheme, the NSA reviews license applications for "information security technologies" covered by ITAR.¹¹

While the agency denies the charges, industry representatives claim that NSA-imposed restrictions are stifling innovation in an area that is increasingly important to the computer industry. They further contend that the controls on the export of encryption technology are forcing U.S. companies to lose markets to foreign competitors. As economics writer Robert Kuttner has noted,

[r]estricting the ability of domestic manufacturers to commercialize and export new technologies no longer assures that advanced technologies will stay out of unfriendly hands: it only diverts the business to

Japanese or European manufacturers who don't share America's view of technological security.

This has the most far-reaching implications for American competitiveness, because it is precisely the most militarily sensitive technologies—super-computers, semiconductor architecture and fabrication, fiber-optics, advanced machine tools, cryptography—that are also key to the competitiveness of America's commercial industry.¹²

Considerations of "national security" can also play a role in the patent system and inhibit the technological innovation that system is intended to foster. The Invention Secrecy Act, a little-known provision enacted in 1952 (the year of NSA's birth), authorizes the Commissioner of Patents and Trademarks to withhold a patent and order that an invention be kept secret "for such period as the national interest requires." Violation of a patent secrecy order is punishable by two years' imprisonment and a \$10,000 fine.¹³ As a Justice Department representative told a congressional subcommittee in 1980, "[w]hat the Invention Secrecy Act says in effect is that there are some inventions that are too dangerous to be disclosed in the way that a patent normally discloses the invention"¹⁴

The number of secrecy orders issued under the Invention Secrecy Act remained relatively constant from 1952 until 1979. Since then, the number of active secrecy orders has increased: a total of 4,685 orders were in effect in 1986 compared with 3,513 in 1979.¹⁵ While information concerning the substance of patent secrecy orders is obviously difficult to obtain, cryptographic technology clearly has been the subject of many such orders issued at the insistence of NSA.¹⁶ These restrictions in effect exempt cryptography from the underlying purpose of the patent system: to "stimulate ideas and the eventual development of further significant advances in the art."¹⁷ NSA's objective has been to suppress, rather than stimulate, advances in civilian cryptography.

NSA Involvement in the Development of Security Standards

As noted, Congress was cognizant of NSA's propensity toward extreme secrecy when it passed

the Computer Security Act and sought to remove the impediments to technological innovation in the civilian sector. Congress specifically intended to "greatly restrict" the influence of the military intelligence agencies "while at the same time providing a statutory mandate for a strong security program headed up by [NIST], a civilian agency."¹⁸ The House Report on the legislation noted that NSA's involvement in the development of civilian computer standards

could have a chilling effect on the vigorous research and development that is on-going in the academic community and our domestic computer industry. This industry has been one of the most viable segments of our economy. Its rapid technological advances have been due in large part to being free to openly exchange ideas without government interference. NSA's inherent tendency to classify everything at its highest level is bound to conflict with this broader goal.

The development of the digital signature standard is, to a large extent, the first real test of the Computer Security Act. Unfortunately, information that has recently come to light suggests that the barrier Congress sought to erect between the civilian and military agencies can easily be breached.

The Federal Register notice announcing the proposed DSS last August made no explicit reference to NSA and clearly implied that NIST had developed the standard. In an effort to analyze the federal standard setting process, Computer Professionals for Social Responsibility ("CPSR") submitted a Freedom of Information Act request to NIST for records related to DSS. In response to the request, the agency initially asserted that

all of the materials related to the evaluation of technology in choosing a digital signature standard for computer security are documents that are advisory and predecisional in nature, and are therefore exempt from disclosure under [FOIA]. In addition, some of the materials pertain to pending patent applications and are withheld under [FOIA] . . . [and] are also protected under the provisions of [patent law].¹⁹

After CPSR filed suit in federal court to compel disclosure of the DSS materials, NIST

acknowledged for the first time that the bulk of relevant documents in its possession in fact originated with NSA—142 pages of material were created by NIST while 1,138 pages were created by NSA.²⁰ For reasons not explained by the agency, NIST dropped its FOIA exemption claims and released 140 pages of its own material and referred the remaining documents to NSA for processing.

In response to news media scrutiny, NSA has now also acknowledged the leading role it played in developing the proposed DSS. In a letter to *MacWeek* magazine, NSA's Chief of Information Policy acknowledged that the agency "evaluated and provided candidate algorithms including the one ultimately selected by NIST."²¹ While NSA steadfastly insists that its role in developing the digital signature standard is consistent with the letter of the Computer Security Act, the fact that the agency actually "provided" the DSS algorithm to NIST raises questions as to whether the spirit of the legislation has been followed.

At least one authoritative observer does not believe it has. Rep. Jack Brooks, who was a driving force behind the Computer Security Act while serving as Chairman of the House Government Operations Committee (and who now serves as Chairman of the Judiciary Committee), recently held hearings on DSS. He noted that

[u]nder the Computer Security Act of 1987, the Department of Commerce [through NIST] has primary responsibility for establishing computer security standards including those dealing with cryptography. However, many in industry are concerned that in spite of the Act, the NSA continues to control the Commerce Department's work in this area. For example, Commerce (at the urging of the National Security Agency) has proposed a "digital signature standard" (DSS) that has been severely criticized by the computer and telecommunications industry.²²

The criticism of DSS alluded to by Rep. Brooks goes to the heart of the matter—whether NSA's involvement in the standard setting process has resulted in the adoption of a flawed standard. Comments submitted to NIST by industry and academic cryptography experts were overwhelmingly critical of the proposed DSS. The

vast majority of these experts expressed the view that the proposed standard is inferior to the established and widely used RSA public-key technology, which many have characterized as the *de facto* international standard.²³

Professor Martin Hellman of Stanford University, the co-inventor of public-key cryptography, wrote that he was "deeply concerned by faults in the technical specifications of the proposed DSS and by its development process." He noted that

NIST has lost considerable credibility with the non-military cryptographic research community and, unless the revision process of DSS is carried out in a much more rapid and open fashion, NIST is likely to become totally ineffective in the setting of cryptographic standards.²⁴

NIST documents released to CPSR under the Freedom of Information Act suggest that the agency's own experts recognized the superiority of the existing RSA technology and its status as an emerging *de facto* authentication standard. An internal NIST evaluation of existing technology conducted in late 1989 noted that the RSA technique is "widely known and widely used" and is "a most versatile public-key cryptosystem."²⁵ Indeed, *IEEE Spectrum* magazine recently reported that the RSA technique

had been readied by NIST as the [federal] standard for several months and was dropped in December 1989 with no alternative in sight. Not until early spring of 1991 did NSA present the algorithm of choice to NIST. Even on background, sources declined to detail reasons behind the decision, although one mentioned that legitimate national security factors had come into play.²⁶

The questions surrounding DSS—both technical and procedural—are so significant that even NIST's Computer System Security and Privacy Advisory Board has expressed reservations about the proposed standard. The Board has called for a "national level public review" of cryptography policy and has deferred approval of the proposed DSS "pending progress on the national review."²⁷ The Undersecretary of Commerce for Technology, Dr. Robert M. White, agreed with the Board's

recommendation and called upon NIST to organize public workshops on cryptography issues.

This review of national cryptography policy comes at a critical time. In the Cold War atmosphere that prevailed for 45 years, cryptography was seen as a vital national interest and most policymakers were willing to permit the National Security Agency and the military establishment to maintain a monopoly in the field. With the end of the Cold War, the military and intelligence considerations have changed. Indeed, Congress recognized the need for reform when it enacted the Computer Security Act in 1987, even before the demise of the Soviet Union.

Electronic communications are now widely used in the civilian sector and have become an integral

component of the global economy. Computers store and exchange an ever increasing amount of highly personal information, including medical and financial data. In this electronic environment, the need for privacy-enhancing technologies is apparent. Communications applications such as electronic mail and electronic funds transfers require secure means of encryption and authentication—goals that can be achieved only through the robust development and dissemination of cryptographic technology free of military interference. To that end, the role of the National Security Agency in civilian cryptography should be eliminated and NIST should be granted the authority and resources to assist, rather than hinder, the development of civilian cryptography in the United States.

Notes

¹ 56 Fed. Reg. 42981 (August 30, 1991).

² "Lynn McNulty on Infosecurity Standards: A Talk with NIST's Protection Point Man," *ISPNews*, (September/October 1992) at 6.

³ See Wright, *The Law of Electronic Commerce* (Little, Brown 1991) at 192-193.

⁴ 56 Fed. Reg. 42981 (August 30, 1991).

⁵ See "The Computer Security Act of 1987 (P.L. 100-235) and the Memorandum of Understanding Between the National Institute of Standards and Technology (NIST) and the National Security Agency (NSA)," the Subcommittee on Legislation and National Security, Committee on Government Operations, House of Representatives, May 4, 1989 (testimony of Marc Rotenberg, CPSR Washington Office Director) reprinted in *Military and Security Control of Computer Security Issues*, 101st Cong., 1st Sess. (1989) at 80.

⁶ H. Rep. No. 153 (Part 2), 100th Cong., 1st Sess. 21 (1987).

⁷ See generally Kahn, *The Codebreakers* (Macmillan 1967).

⁸ Burnham, *The Rise of the Computer State* (Random House 1980), at 126. See generally Bamford, *The Puzzle Palace* (Houghton Mifflin 1982); "The National Security Agency and Fourth Amendment Rights," Hearings before the Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities, 94th Cong., 1st Sess. (1975).

⁹ 22 CFR Parts 120-130.

¹⁰ See generally, Greguras and Black, "The Encryption Export Maze: Red Tape, Requirements, Restrictions," *INFOSecurity Product News* (June 1992).

¹¹ Adam, "Cryptography = Privacy?," *IEEE Spectrum*, August 1992 at 34 (reprinted statement of NSA).

¹² Kuttner, "Spooks and Science: An American Dilemma," *The Washington Post*, August 20, 1989, at B8. See, also Kuttner, "How 'National Security' Hurts National Competitiveness," *Harvard Business Review*, January - February 1991, at 140.

¹³ 35 U.S.C. § 181 *et seq.*

¹⁴ "The Government's Classification of Private Ideas," Hearings before a Subcommittee of the House Committee on Government Operations, 96th Cong., 2d Sess. (1980) (hereinafter cited as "Private Ideas") at 258 (testimony of H. Miles Foy, Office of Legal Counsel, Department of Justice).

¹⁵ Hausken, "The Value of a Secret: Compensation for Imposition of Secrecy Orders under the Invention Secrecy Act," 119 *Military Law Review* (Winter 1988) at 202 n.10 (446 new orders were issued in 1986 compared with 293 in 1979).

¹⁶ See "Private Ideas" at 406-431; see also Gilbert, "Patent Secrecy Orders: The Unconstitutionality of Interference in Civilian Cryptography under Present Procedures," 22 *Santa Clara Law Review* 325 (1982).

¹⁷ *Kewanee Oil Co. v. Bicron Corp.*, 416 U.S. 470, 481 (1974).

¹⁸ H. Rep. No. 153 (Part 2), 100th Cong., 1st Sess. 7 (1987).

¹⁹ Letter from NIST to CPSR dated September 11, 1991.

²⁰ *CPSR v. NIST*, Civil Action No. 92-0972 (D.D.C.) (agency affidavits filed in support of motion to stay proceedings).

²¹ Letter from Michael S. Conn (NSA) to Mitch Ratcliffe (MacWeek), October 31, 1991.

²² Opening Statement of Rep. Jack Brooks, *Threat of Foreign Economic Espionage to U.S. Corporations*, House Judiciary Subcommittee on Economic and Commercial Law, May 7, 1992 at 2.

²³ See, e.g., Comments submitted to NIST by Fischer International Systems Corp., dated November 26, 1991. See also "Debating Encryption Standards," *Communications of the ACM*, July 1992 at 34 ("After years of testing and proven reliability, RSA is now used by the majority of software makers around the world, including IBM, Apple, Lotus, Sun and Microsoft").

²⁴ Comments submitted to NIST by Professor Martin E. Hellman, dated November 12, 1991, reprinted in *Communications of the ACM*, July 1992 at 47-49.

²⁵ Memorandum from Roy Saltman to Lynn McNulty dated December 22, 1989.

²⁶ Adam, "Cryptography = Privacy?," *IEEE Spectrum*, August 1992 at 29.

²⁷ Computer System Security and Privacy Advisory Board, Resolutions No. 1 and 3, March 18, 1992.

**Computer Professionals for Social Responsibility
Washington Office
Suite 303
666 Pennsylvania Avenue, S.E.
Washington, DC 20003**

May 6, 1993

Contact:
David Sobel
(202) 544-9240

Documents Show NSA Dominance of Civilian Computer Security

Less than three weeks after the White House announced a controversial initiative to secure the nation's electronic communications with government-approved cryptography, newly released documents raise serious questions about the process that gave rise to the administration's proposal. The documents, released by the National Institute of Standards and Technology (NIST) in response to a Freedom of Information Act lawsuit, suggest that the super-secret National Security Agency (NSA) dominates the process of establishing security standards for civilian computer systems in contravention of the intent of legislation Congress enacted in 1987.

The released material concerns the development of the Digital Signature Standard (DSS), a cryptographic method for authenticating the identity of the sender of an electronic communication and for authenticating the integrity of the data in that communication. NIST publicly proposed the DSS in August 1991 and initially made no mention of any NSA role in developing the standard, which was intended for use in unclassified, civilian communications systems. NIST finally conceded that NSA had, in fact, developed the technology after Computer Professionals for Social Responsibility (CPSR) filed suit against the agency for withholding relevant documents. The proposed DSS was widely criticized within the computer industry for its perceived weak security and inferiority to an existing authentication technology known as the RSA algorithm. Many observers have speculated that the RSA technique was disfavored by NSA because it was, in fact, more secure than the NSA-proposed algorithm and because the RSA technique could also be used to encrypt data very securely.

The newly-disclosed documents -- released in heavily censored form at the insistence of NSA -- suggest that NSA was not merely involved in the development process, but dominated it. NIST and NSA worked together on the DSS through an intra-agency Technical Working Group (TWG). The documents suggest that the NIST-NSA relationship was contentious, with NSA insisting upon secrecy throughout the deliberations. A NIST report dated January 31, 1990, states that

(more)

The members of the TWG acknowledged that the efforts expended to date in the determination of a public key algorithm which would be publicly known have not been successful. It's increasingly evident that it is difficult, if not impossible, to reconcile the concerns and requirements of NSA, NIST and the general public through using this approach.

The civilian agency's frustration is also apparent in a July 21, 1990, memo from the NIST members of the TWG to NIST director John W. Lyons. The memo suggests that "national security" concerns hampered efforts to develop a standard:

THE NIST/NSA Technical Working Group (TWG) has held 18 meetings over the past 13 months. A part of every meeting has focused on the NIST intent to develop a Public Key Standard Algorithm Standard. We are convinced that the TWG process has reached a point where continuing discussions of the public key issue will yield only marginal results. Simply stated, we believe that over the past 13 months we have explored the technical and national security equity issues to the point where a decision is required on the future direction of digital signature standards.

An October 19, 1990, NIST memo discussing possible patent issues surrounding DSS noted that those questions would need to be addressed "if we ever get our NSA problem settled."

Although much of the material remains classified and withheld from disclosure, the "NSA problem" was apparently the intelligence agency's demand that perceived "national security" considerations take precedence in the development of the DSS. From the outset, NSA cloaked the deliberations in secrecy. For instance, at the March 22, 1990, meeting of the TWG, NSA representatives presented NIST with NSA's classified proposal for a DSS algorithm. NIST's report of the meeting notes that

The second document, classified TOP SECRET CODEWORD, was a position paper which discussed reasons for the selection of the algorithms identified in the first document. This document is available at NSA for review by properly cleared senior NIST officials.

In other words, NSA presented highly classified material to NIST justifying NSA's selection of the proposed algorithm -- an algorithm intended to protect and authenticate unclassified information in civilian computer systems. The material was so highly classified that "properly cleared senior NIST officials" were required to view the material at NSA's facilities.

(more)

These disclosures are disturbing for two reasons. First, the process as revealed in the documents contravenes the intent of Congress embodied in the Computer Security Act of 1987. Through that legislation, Congress intended to remove NSA from the process of developing civilian computer security standards and to place that responsibility with NIST, a civilian agency. Congress expressed a particular concern that NSA, a military intelligence agency, would improperly limit public access to information in a manner incompatible with civilian standard setting. The House Report on the legislation noted that NSA's

natural tendency to restrict and even deny access to information that it deems important would disqualify that agency from being put in charge of the protection of non-national security information in the view of many officials in the civilian agencies and the private sector.

While the Computer Security Act contemplated that NSA would provide NIST with "technical assistance" in the development of civilian standards, the newly released documents demonstrate that NSA has crossed that line and dominates the development process.

The second reason why this material is significant is because of what it reveals about the process that gave rise to the so-called "Clipper" chip proposed by the administration on April 16. Once again, NIST was identified as the agency actually proposing the new encryption technology, with "technical assistance" from NSA. Once again, the underlying information concerning the development process is classified. DSS was the first test of the Computer Security Act's division of labor between NIST and NSA. Clipper comes out of the same "collaborative" process. The newly released documents suggest that NSA continues to dominate the government's work on computer security and to cloak the process in secrecy, contrary to the clear intent of Congress.

On the day the Clipper initiative was announced, CPSR submitted FOIA requests to key agencies -- including NIST and NSA -- for information concerning the proposal. CPSR will pursue those requests, as well as the pending litigation concerning NSA involvement in the development of the Digital Signature Standard. Before any meaningful debate can occur on the direction of cryptography policy, essential government information must be made public -- as Congress intended when it passed the Computer Security Act. CPSR is committed to that goal.

Selected NSA/NIST Documents Concerning the Development
of the Digital Signature Standard (DSS)

Released in

Computer Professionals for Social Responsibility

v.

National Institute of Standards and Technology

Civil Action No. 92-0972 (D.D.C.)



UNITED STATES DEPARTMENT OF COMMERCE
Office of the General Counsel
Washington, D.C. 20230

APR 22 1993

David Sobel, Esq.
Computer Professionals
for Social Responsibility
666 Pennsylvania Ave., S.E.
Suite 303
Washington, D.C. 20003

Re: Freedom of Information Act Appeal of
October 1, 1991 for records on choosing a
Digital Signature Standard

Dear Mr. Sobel:

This supplements the June 22, 1992 letter to you on the above matter. NSA has now completed its review of two categories of documents: (1) documents with attachments that originated at NSA, and (2) documents with references to NSA or NSA staff members or containing other NSA information.

After receiving the results of NSA's review, the Department has determined which of the documents should be released and which should be withheld based on one or more exemptions under the Freedom of Information Act (5 U.S.C. § 552) (FOIA). Also, some material is not being provided because it is nonresponsive to the request. The documents being released in their entirety or in part are enclosed (with portions being withheld deleted).

Material is being withheld by the Department, on its own determination, based on the attorney-client privilege incorporated in exemption (b)(5) of the FOIA. Other material is being withheld by the Department, on its own determination and at the request of NSA, on the basis of the deliberative process privilege incorporated in exemption (b)(5) of the FOIA. Also, at NSA's request, the Department is withholding additional documents or portions thereof pursuant to exemptions (b)(1), (b)(3) (based on 18 U.S.C. § 798 and 50 U.S.C. § 402 note), and the attorney-client and attorney work-product privileges incorporated in exemption (b)(5).

This is the final decision of the Department of Commerce with respect to the two categories of documents above.

Sincerely,

Barbara S. Fredericks
Assistant General Counsel
for Administration

Enclosures

We feel that the time has come to develop a set of public-key based Federal Information Processing Standards. Several factors have lead us to this conclusion.

1. An Internet Advisory Board Privacy Task Force draft Request For Comments (RFC) proposes an RSA based key distribution scheme for the distribution of DES keys which can then be used to encrypt Internet mail. This distribution system will require that public-keys be certified by RSA. Government agencies will consider using this Internet document in lieu of a standard.
2. Public-Key based cryptography has been proposed for the Electronic Data Interchange (EDI) and Computer Aided Acquisition Logistic Support (CALS) programs.
3. An unclassified, public-key based, key distribution system is necessary if the Secure Data Network System (SDNS) protocols are to be widely accepted for Government and commercial applications.
4. The Department of Treasury requested that we develop a public-key standard for key distribution in the Consolidated Data Network (CDN).
5. As an increasingly number of information systems become automated, a digital signature standard is required to replace the written signature. The value of such a standard has been confirmed by the Subcommittee on Automated Information Systems Security (SAISS) in its Retreat Summary/Action Report of November 21, 1988.
6. A public-key based digital signature system, endorsed by the Government, could serve as a useful tool in protecting Government and commercial software against hackers and viruses.

NIST plans to develop the necessary public-key based security standards. We require a public-key algorithm for calculating digital signatures and we also require a public-key algorithm for distributing secret keys. At this time we do not need a public-key algorithm for general data encryption. The algorithms that we use must be public, unclassified, implementable in both hardware or software, usable by Federal Agencies and U.S. based multi-national corporations, and must provide a level of security sufficient for the protection of unclassified, sensitive information and commercial proprietary and/or valuable information.

We would prefer having one public key (assymetric) cryptographic algorithm that does both digital signatures and key distribution. We would like NSA to assist this standards program by evaluating candidate algorithms proposed by NIST and by providing new algorithms when existing algorithms do not meet NIST requirements. We propose this as being the first issue to discuss under paragraph III.5 of the NIST-NSA MOU.



45

MAY 03 1989

MEMORANDUM FOR THE RECORD

From: Lynn McNulty
Associate Director, Computer Security

Subject: First Meeting of the NIST/NSA
Technical Working Group (TWG)

(b)(3)*

On May 5, 1989, the first meeting of the NIST/NSA TWG was held at the NSA Building, Fort Meade, MD. The establishment of this group is authorized in paragraph III.7. of the NIST/NSA Memorandum of Understanding, dated March 24, 1989. The participants in this meeting included:

NIST

Elaine Barker
Dennis Branstad
Lynn McNulty

NSA

[REDACTED]

N.R.

SUBSTANTIVE BUSINESS

The NIST representatives stated that they had two items to bring to the attention of the TWG at this meeting. These were (1) public key cryptography for digital signature and key distribution; and [REDACTED]

[REDACTED] The NIST objectives and requirements for each issue are detailed in the attachments to this memorandum.

Issue I: Public Key

The NSA representatives expressed the opinion that any public key solution provided by NSA must be capable of withstanding close public scrutiny and discussion. In response to a question from a NSA representative, Dennis Branstad stated that NIST planned to utilize public key techniques as a means for protecting digital signatures and for distributing secret keys. NIST does not perceive a requirement for using public key techniques for the encryption of data at this time. Dr. Branstad also stated that NIST desired both hardware and software implementations of public key technology.

A general discussion then followed of the legal and technical issues inherent in the use of a public key strategy to satisfy existing requirements in the unclassified sector. At the conclusion of this discussion NSA agreed to:

- (1) Work with NIST, within the fourteen-day time frame specified in the MOU, to assure a NSA response to this matter.
- (2) Provide a briefing for the NIST team on NSA views on public key systems.
- (b)(3)* (3) Provide NIST representative with a briefing on the [REDACTED]

*Remainder of page
N.R.*



46

May 13, 1989

MEMORANDUM FOR THE RECORD

From: Lynn McNulty *LM*
Associate Director, Computer Security

Subject: Second Meeting of the NIST/NSA
Technical Working Group (TWG)

On May 12, 1989, the second meeting of the NIST/NSA TWG was held at the NSA Building, Fort Meade, MD. The participants in this meeting included:

(b)(3)*

NIST

Elaine Barker
Dennis Branstad
Lynn McNulty

NSA

[REDACTED]

N.R.

DISCUSSION OF ISSUE #1 -- PUBLIC KEY

The TWG conducted a wide ranging discussion of the issues inherent in the use of public key technology within the public sector. This discussion was primarily intended to provide NSA with additional information regarding NIST's concept of how public key technology would be utilized and what options were available for satisfying the NIST requirements. Specific topics discussed included the use of public key for signature verification, EDI applications, key distribution and data encryption. Items of interest expressed during this discussion included:

(b)(3)*

[REDACTED] (NSA) stated that NSA has established an internal committee to address public key issues.

-- Dr. Branstad (NIST) stated that there is a growing need to have a digital signature technique to prevent tampering with software and to trace it to an authorized distributor.

(b)(3)*

[REDACTED] advised the group that there are no export restrictions on the use of public key for hashing or authentication. At the conclusion of this phase of the discussion on public key cryptology, the NSA team leader stated that NSA will make every effort to satisfy the NIST request for assistance in the public key area. NSA will assist in finding the best solution to the problem -- one that will satisfy the greatest number of requirements. The discussion of Issue #1 was suspended in order to allow [REDACTED] of NSA to discuss Issue #2. Due to a conflict in his schedule [REDACTED] could not remain for the entire meeting.

*Remainder of page
N.R.*

RESUMPTION OF THE ISSUE #1 - PUBLIC KEY DISCUSSION

The NSA TWG leader asked NIST to develop a set of evaluation criteria for use in their review of various public key alternatives. A discussion followed of what should be included in any evaluation matrix. Topics discussed included intended uses of public key algorithms; what was to be protected; what were the threats; what types of attacks could be mounted on public key transactions; and what was the anticipated life span of a possible NIST standard for public key.

ACTION ITEMS: NIST will provide NSA with a Public Key evaluation matrix at the next meeting.

NEXT MEETING: It was agreed that the next meeting of the TWG would be held at NSA on Friday May 19, at 0900 hours.

Concurrence:

D. Branstad DB
E. Barker eb

cc: Ray Kammer
James Burrows



(48) (48)

May 20, 1989

MEMORANDUM FOR THE RECORD

From: Lynn McNulty *LM*
Associate Director, Computer Security

Subject: Third Meeting of the NIST/NSA
Technical Working Group (TWG)

On May 19, 1989, the third meeting of the NIST/NSA TWG was held at the NSA Building, Fort Meade, MD. The participants in this meeting included:

(b)(3)*

NIST
Elaine Barker
Dennis Branstad
Lynn McNulty

NSA


*Remainder of page
N.R.*

CONTINUED DISCUSSION OF ISSUE #1--PUBLIC KEY

Dr. Branstad presented to the TWG the public key evaluation matrix that NIST was charged with preparing at second meeting. This document was discussed and some interpretations made as a result of the verbal review conducted by the TWG. The NSA team leader advised NIST personnel that a candidate algorithms would be reviewed against this criteria. In accordance with the commitments stated in the progress reports an interim report will be issued by NSA within thirty days. A schedule for the completion of the full security evaluation candidate algorithms will be provided at this time.

N.R.

Attachments

Concurrence:

D. Branstad DB
E. Barker EB

cc: Ray Kammer
James Burrows

~~CONFIDENTIAL~~

88

19 May 1989

MEMORANDUM FOR James Hearn
NSA DDI

Raymond Kammer
NIST Acting Director

(b)(3)* FROM

[REDACTED]
NSA TWG Team Leader

Lynn McNulty
NIST TWG Team Leader

SUBJECT Status Report on TWG Issue Number 1 (U)

(U) Issue Number 1 (Attachment 1) was presented to the TWG by NIST on May 5, 1989. The TWG met again on May 19 to discuss the issue and to receive briefings on possible algorithms that would meet the NIST requirements.

(U) NSA members requested that NIST establish a set of evaluation criteria against which the algorithms can be evaluated and compared. The requested set of criteria, a list of algorithms and a set of assumptions are contained in Attachment 2.

(b)(1)
(b)(3)* [REDACTED]
(U) NIST stated its desire for one algorithm that will do both digital signature and key distribution.

(b)(5) [REDACTED]
NIST stated that it would be very difficult to support two different algorithm standards where one could suffice. It would also be difficult to support standards contrary to wide user acceptance.

(U) A hashing algorithm is generally used with a digital signature algorithm. A hashing algorithm is used to compute a digital representation of a message to be signed that is shorter than the message itself. The digital representation, called a Hash, is signed and accompanies the digital message. A receiver of the digital message computes a Hash on the received message and compares it with the received signed Hash using the Digital Signature Algorithm. The signature and the message are considered authentic if the computed Hash compares correctly with the received signed Hash.

~~CONFIDENTIAL~~

Classified By NSA/CSS 123-2

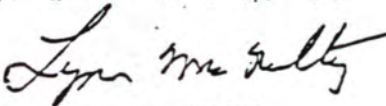
Declassify On: Originating Agency's Determination Authority

~~CONFIDENTIAL~~

(U) NSA stated that they would evaluate the candidate algorithms against the set of criteria provided by NIST. The matrix of candidate algorithms against criteria will be completed in 30 days. Within 30 days thereafter, NSA will present a schedule for the completion of a full security evaluation of the selected system.

(b)(3)


NSA TWG Team Leader


LYNN MCNULTY
NIST TWG Team Leader

2 Attachments

~~CONFIDENTIAL~~

July 11, 1989



UNITED STATES DEPARTMENT OF COMMERCE
National Institute of Standards and Technology
[formerly National Bureau of Standards]
Gaithersburg, Maryland 20899

17

~~SECRET~~

MEMORANDUM FOR THE RECORD

SUBJECT: Fourth Meeting of the NIST/NSA
Technical Working Group (TWG)

On July 10, 1989 the fourth meeting of the NIST/NSA TWG was held at the NSA Building, Fort Meade, MD. The participants in this meeting included:

NIST

Elaine Barker
Dennis Branstad
Lynn McNulty

NSA

[REDACTED]

DISCUSSION OF ISSUE #1 -- PUBLIC KEY

[REDACTED] began the meeting by handing out three documents which described the status of the evaluations of candidate public key algorithms conducted to date by NSA in response to the request by NIST stated in the Issue #1 paper referred to the TWG. (Note: Two of these summary documents are classified SECRET. When all summary documents are attached to this memorandum it is a SECRET document.) The following factors were discussed regarding Issue #1:

[REDACTED]

SECRET

(Regrade to Unclassified upon separation from
CLASSIFIED ATTACHMENT)

N.R.

Concurrence:

D. Branstad

E. Barker

D. Branstad
E. Barker

cc: Ray Kammer
James Burrows

Attachments (3 - 1 & 2 classified SECRET)

~~SECRET~~



UNITED STATES DEPARTMENT OF COMMERCE
National Institute of Standards and Technology
[formerly National Bureau of Standards]
Gaithersburg, Maryland 20899

September 22, 1989

49

MEMORANDUM FOR THE RECORD

SUBJECT: Seventh Meeting of the NIST/NSA
Technical Working Group (TWG)

(u) On September 22, 1989 the seventh meeting of the NIST/NSA TWG was held at the BDM facility in Columbia, MD. The participants in this meeting included:

NIST

NSA

Elaine Barker
Dennis Branstad
Lynn McNulty

DISCUSSION OF ISSUE #1- PUBLIC KEY

(b)(3)* [redacted] briefed the TWG on the progress achieved to date by NSA in responding to the NIST request for assistance in developing a standard for the use of public key cryptography for unclassified applications. His briefing included the following points of interest:

(b)(1)
(b)(3)* [redacted]

(b)(5) [redacted]

(u) A general discussion of the topics covered in Mr. Marshall's briefing followed. Significant items covered in this discussion included:

(u) • Method of Publishing the Public Key Standard. Dr. Branstad stated that NIST intends to use NSA's final evaluation report on developing a public key standard that will be made available for public comment

~~SECRET~~

~~SECRET~~

-2-

(b)(3)* [before final publication. NIST will assure that this document will be carefully worded so as not to contain any real or implied liability to the government concerning the strength of the algorithm. [reported that there had been some discussions within NSA regarding their public participation in any meetings or symposiums on the future public key standard.

(b)(3)* (u) [Federal Agency Use of the Public Key Standard. [stated that some NSA personnel believe that NIST should advocate immediate use of the public key standard within the unclassified sector of the Federal government. This would demonstrate to potential skeptics that NIST had confidence in the strength and reliability of this algorithm. This would also stimulate the development of the market for products that implement the standard. The discussion included several potential candidates for the use of the future standard.

(u) [Exportability. NSA personnel acknowledged the potential political and technical problems regarding the exportability issue. The Agency hopes that the algorithm adopted for unclassified Federal agency use will also satisfy export restrictions.

(b)(3)* (u) [Completion Date for NSA Work on Issue #1. [stated that NSA will provide NIST with a formal response to Issue #1 by December 1989. Additional staff resources have been added to the effort to assure completion by this date.

(u) ACTION ITEMS: As a result of the discussion it was agreed that NIST would accept two action items for the next TWG meeting. These included:

Action Item 7-1. NIST will develop a set of intended applications for the use of public key technology within the unclassified segment of the government.

Action Item 7-2. NIST will prepare an initial draft of a press release and Federal Register Notice announcing the release for public comment of the draft public key standard.

Remainder of page, next page and
2 attachments
N.R.



November 23, 1989

51

MEMORANDUM FOR THE RECORD

SUBJECT: Ninth Meeting of the NIST/NSA
Technical Working Group (TWG)

(4) On November 22, 1989, the ninth meeting of the NIST/NSA TWG was held in the Office of the Associate Director for Computer Security at the National Institute of Standards and Technology, Gaithersburg, Maryland. The participants in this meeting included:

(b)(3)*

NIST
Elaine Barker
Dennis Branstad
Lynn McNulty

NSA
[REDACTED]
[REDACTED]
[REDACTED]

(b)(3)*

DISCUSSION OF ISSUE #1--PUBLIC KEY.

[REDACTED] advised the NIST representatives that NSA would not be able to meet the previously agreed upon December 15 deadline for providing a response to the request for assistance in the development of a public key standard. The NSA technical staff working on the public key problem will report their findings to the Director of NSA in early January. NIST will be advised of the NSA position on public key sometime after this date.

(b)(1)

(b)(3)**

(b)(5)

[REDACTED]
He also quoted one NSA officer as stating that this was the most "interesting" research problem he had worked on during his career with the agency. [REDACTED]

The NIST representatives expressed their disappointment at this latest slippage in receiving a response from NSA on the Public Key issue. Mr. McNulty expressed the opinion that this issue has been characterized by continuing delays in receiving a response from NSA. Dr. Branstad stated that this will force NIST to reexamine its strategy on this matter. Given the pressures upon NIST to provide leadership in the public key field, consideration must be given by NIST to initiating the public participation process on a proposed public key standard before mid-January. He also requested a briefing at the next TWG meeting on the technical issues identified to date with respect to various public key algorithms. The NSA representative agreed to try and make the necessary arrangements for a briefing. (NSA ACTION ITEM 9-1) The NIST representative stated that this unanticipated delay will be referred to senior NIST officers along with a recommended course of action.

page 2, 3 + 4
N. R.

SECRET



December 19, 1989

MEMORANDUM FOR THE RECORD

SUBJECT: Tenth Meeting of the NIST/NSA
Technical Working Group (TWG)

On December 18, 1989, the tenth meeting of the NIST/NSA TWG was held at the NSA Building, Fort Meade, Maryland. The participants in the meeting included:

(b)(3)*
NIST
Elaine Barker
Dennis Branstad
Lynn McNulty
Ray Kammer (Acting Director,
NIST)

NSA

Jim Hearn (Deputy Director,
INFOSEC)

BRIEFING ON NSA'S TECHNICAL INVESTIGATION OF PUBLIC KEY ALGORITHMS SUITABLE FOR UNCLASSIFIED APPLICATIONS.

The primary purpose of this meeting was the presentation of a briefing on the current status of NSA's technical investigations of various public key algorithms. These efforts were undertaken pursuant to the request submitted from Mr. Kammer to Dr. Hearn in May 1989. (NOTE: Reference TWG Issue Paper #1 and subsequent minutes of the TWG for additional details of the analysis accomplished by NSA). This briefing was conducted by Mr. Ed Donoghue, Chief

(b)(3)*
Due to the fact that the great majority of this meeting was held at the TOP SECRET SI level, these minutes do not reflect the full extent of the discussions among the participants. No classified minutes have been prepared. The following is an unclassified summary of this meeting.

Dr. Hearn opened the discussion by stating that he believed that it was an appropriate time for NIST and NSA personnel to receive a detailed briefing on the technical work that has been accomplished to date by NSA to satisfy NIST's request for assistance in the field of public key cryptography. He then turned the meeting over to [redacted] They provided detailed information on the progress made to date to evaluate various algorithms against the functional requirements previously identified by NIST.

(b)(5)
Signature [redacted]

N.R.

Mr. McNulty expressed the opinion that a major DOD program (CALS) was projecting the use of RSA as the standard public key algorithm. This would effectively place a major element within DOD at variance with any proposal coming out of the TWG process and placed into the open standards process.

It was agreed that a subcommittee of the TWG would be formed to develop a strategy for taking the work of the TWG and carrying this forward into the standards arena. The principals tasked the TWG members with preparing a draft implementation plan for discussion at the next TWG meeting. (NIST ACTION ITEM #1)

The next meeting of the TWG was scheduled for the week of January 8.

Prepared by:

L. McNulty LM

Concurrence:

D. Branstad DKB

E. Barker EB

cc: Ray Kammer
James Burrows

3 page attachment N.R.

54

January 31, 1990

MEMORANDUM FOR THE RECORD

(u) SUBJECT: Twelfth Meeting of the NIST/NSA
Technical Working Group (TWG)

(b)(3)* On January 31, 1990, the twelfth meeting of the NIST/NSA TWG was held in the NSA Building at Fort Meade, MD. The participants in this meeting were:

NIST
Elaine Barker
Dennis Branstad
Lynn McNulty

NSA
[REDACTED]

N.R.

(u) [REDACTED] presented Dr. Hearn's concerns regarding the public key algorithm proposal discussed at the previous meetings. Dr. Hearn's primary concern was that [REDACTED]

(b)(5)

[REDACTED] Dr. McNulty felt that the proposal was also "out of line" with the rest of the world.

(b)(5)

(u) Dr. Branstad expressed the opinion that while he preferred a single, publicly known standard, this could be a "fall back" position if an acceptable algorithm which could be public could not be agreed upon. His thoughts were that the algorithm should be registered without parameters and that the recommended parameters for different uses (e.g., government use, export use) should be made part of a "profile" similar to one used in GOSIP.

(u) The members of the TWG acknowledged that the efforts expended to date in the determination of a public key algorithm which would be publicly known have

~~SECRET~~

~~SECRET~~

not been successful. It's increasingly evident that it is difficult, if not impossible, to reconcile the concerns and requirements of NSA, NIST and the general public using this approach.

N.R. [REDACTED]

In addition, Dr. Branstad felt that the "signature plus" package (i.e., digital signature plus hashing plus key management) should be a separate package, requiring the development of a separate standard. He felt that the use of one (or perhaps two) publicly known algorithms would be desirable which could be implemented in software. There would be a "profile" containing parameters, etc. for government use. He does not believe there is any need for making the digital signature and hashing algorithms secret. [REDACTED] stated that NSA is currently studying the concept of allowing the algorithms for this package to be public with no restrictions.

(b)(3)* (u) The TWG agreed that the following activities should be pursued:

(b)(3)* (u) o the formation of a joint NSA/NIST group to discuss policy issues. [REDACTED] and Mr. McNulty will attempt to initiate this effort in the next week to prepare a charter statement for the group;

N.R. [REDACTED]

(u) Dr. Branstad requested that NSA evaluate the SNEFERU II algorithm for (hashing) and expressed the opinion that the hashing algorithm only needed to be as good as the digital signature algorithm. He also requested a technical briefing on hashing (i.e., threats, etc.).

page 3 N.R.

~~SECRET~~

February 8, 1990

55

MEMORANDUM FOR THE RECORD

SUBJECT: Thirteenth Meeting of the NIST/NSA
Technical Working Group (TWG)

(b)(3)* On February 8, 1990, the thirteenth meeting of the NIST/NSA TWG was held in the NSA Building at Fort Meade, MD. The participants in this meeting were:

NIST
Elaine Barker
Dennis Branstad

NSA
[REDACTED]

N.R.

One goal for the Digital Signature Plus (DSP) system (signature and hashing algorithms plus key/certificate exchange) is to allow a software implementation. NSA is still studying the various candidate solutions for this problem.

(b)(3)* All TWG members agreed that a "show of progress" on this issue was required. [REDACTED] expressed the opinion that generic standards could easily be developed for [REDACTED] Digital Signature Plus systems. A registry of algorithms could be used for algorithm specifications and then profiles could be developed for specific applications. Dr. Branstad felt that this approach was only possible if the algorithms are known before the standards are initiated. He stated that such standards must be designed to handle both the current publicly known algorithms and the government designed algorithms.

N.R.

Remainder of page and next 3 pages
N.R.



March 26, 1989

MEMORANDUM FOR THE RECORD

SUBJECT: Fifteenth Meeting of the NIST/NSA
Technical Working Group (TWG)

On March 22, 1990, the fifteenth meeting of the NIST/NSA TWG was held at the NSA Building, Fort Meade, MD. The participants in the meeting included:

NIST

Elaine Barker
Dennis Branstad
Lynn McNulty

NSA

N.R

PUBLIC KEY CRYPTOGRAPHY - ISSUE #1.

(b)(3)* [redacted] distributed two documents to the NIST representatives. The first, classified CONFIDENTIAL, contained NSA's proposal to NIST containing a cryptographic algorithm and a hashing function which can be used as bases for an unclassified standard for digital signatures used by the U.S. Government. The document presents the results of the technical investigation of public key cryptographic algorithms conducted by NSA pursuant to the NIST request of May 5, 1989. [redacted] stated that it is NSA's intent to promptly initiate declassification action on this document. A copy of this document will be included as Attachment #2 upon its declassification by NSA.

The second document, classified TOP SECRET CODEWORD, was a position paper which discussed reasons for the selection of the algorithms identified in the first document. This document is available at NSA for review by properly cleared senior NIST officials.

Following a review of these documents by the NIST representatives, a discussion transpired on the technical aspects of the NSA recommendations for the signature and hashing algorithms.

(b)(5)

[redacted]

patents held by the Public Key Partners consortium was also discussed. It was agreed that this matter will require additional examination by the NSA and NIST legal staffs.

(b)(5)

[REDACTED]

N.R.

Attachment
N.R.

~~FOR OFFICIAL USE ONLY~~

May 1, 1990

(u) MEMORANDUM FOR Raymond Kammer
Deputy Director, NIST

FROM: Lynn McNulty
Associate Director for
Computer Security, NCSL

(u) SUBJECT: Status of NIST/NSA Activities to Develop Public Key
Cryptographic Standards and Other Matters of Common Concern

(u) BACKGROUND

NIST and NSA have held fifteen TWG meetings over the past year concerning four issues that have been formally proposed for discussion. These are:

--ISSUE #1. Development of Public Key Cryptography Based Standards.
NIST requested NSA assistance in evaluating existing public domain algorithms and in providing new algorithms when existing algorithms do not meet NIST requirements.

N.R.

(u) STATUS OF ISSUES:

--Technical Issue #1. (Public Key) Considerable effort has been expended to date on the public key issue. Every one of the fifteen TWG meetings has dealt with this subject. Our initial request, dated May 5, 1989, asked for NSA assistance in developing public key standards to perform: (1) signature; (2) hashing; and (3) key distribution functions. On March 26, we received a classified proposal for digital signature and hashing algorithms. We did not receive an unclassified version of this document until April 26. NSA recommended a key distribution technique which we could not accept because of its inherent technical deficiencies.

(b)(5)

o The NSA proposal is presently being studied by our technical experts. No meaningful work was accomplished until the receipt of the unclassified version of the document. It is anticipated that as a result of our examination of the proposal, it will be necessary to have an additional technical exchange with the NSA public key technical experts.

o We also need to accomplish a legal review of the patent license issue. The recent establishment of the Public Key Partnership Corporation further complicates this complex problem.

o If these initial questions are satisfactorily resolved, the digital signature/hashing proposal will be sent to a limited number of recognized experts outside of the government for their independent evaluation and review.

o Following this "sanity check" the proposed standard will be published in the Federal Register for public comment.

Remainder of page and next page

N. R



May 8, 1990

MEMORANDUM FOR THE RECORD

SUBJECT: Sixteenth Meeting of the NIST/NSA
Technical Working Group (TWG)

On May 7, 1990, the sixteenth meeting of the NIST/NSA TWG was held at the NSA Building, Fort Meade, MD. The participants in the meeting included:

(b) (3)*

NIST
Elaine Barker
Dennis Branstad
Lynn McNulty

NSA
[REDACTED]

Remainder of page and
next page.
N.R.

N.R.

N.R.

PUBLIC KEY CRYPTOGRAPHY (ISSUE NO. 1)

(b)(3)* NIST outlined the planned approach for reviewing and proposing the Public Key Signature Algorithm (PKSA) standard. Dr. Branstad stated that he had spoken with Dr. Jim Omura from Cylink and Mr. Jim Bidzos from RSA Data Security Inc. regarding the new Public Key Partnership. He stated his desire that all parties who have purchased licenses for public key cryptography that may be affected by a PKSA standard would be able to use the standard without additional licensing cost. [REDACTED] stated that any organization in the government did not need a license for either the RSA or Diffie-Hellman licenses because the government had financially supported the work leading to the patents. [REDACTED]

(b)(3) [REDACTED] Dr. Branstad stated that he felt the patent issue should be clarified with those organizations known to be affected by a potential standard prior to the announcement. All other organizations that may be affected by the proposed standard would have an opportunity at a later time to clarify their position.

(b)(3) A meeting of NIST and NSA is scheduled on May 17 to discuss certain technical merits of the hashing and signature algorithms. This meeting will be held at NIST. [REDACTED] and Dr. Branstad stated an interest in participating in that meeting.

N.R. [REDACTED] stated that NSA had not forgotten about the request but that the PKSA had been given the highest priority by the TWG and NSA. [REDACTED]

(b)(3)* [redacted] stated that he thought NSA would be willing to provide legal assistance on the patent issues. [redacted] is a NSA patent attorney and would be contacted. [redacted] thought that Mr. Schnorr had patented a variant of the El Gamal signature to increase its efficiency. Mr. McNulty stated that additional legal assistance would be appreciated.

Dr. Branstad stated that he still wanted NSA's answers to the questions NIST raised last summer regarding the candidate public key cryptographic algorithms. These questions included comparative security, efficiency, ease of implementation and use. [redacted] stated that they would still work on this (NSA ACTION 16-1).

NEXT TWG MEETING

No date for the next meeting was established.

Prepared by: Dennis K. Branstad
Dennis K. Branstad

Concurrence:

Elaine Barker
Elaine Barker
F. Lynn McNulty
F. Lynn McNulty

Attachment

cc: JLyons, RKammer, JBurrows, SKatzke

~~SECRET~~

DEPARTMENT OF COMMERCE
/ Standards and Technology
JSSS

36

July 24, 1990

MEMORANDUM FOR John W. Lyons
Director, NIST

(u) Through: Raymond G. Kammer
Deputy Director, NIST

James H. Burrows
Director, NCSL

From: Dennis K. Branstad, F. Lynn McNulty
NIST Members of the NIST/NSA Technical Working Group

(u) The NIST/NSA Technical Working Group (TWG) has held 18 meetings over the past 13 months. A part of every meeting has focused on the NIST intent to develop a Public Key Standard Algorithm Standard. We are convinced that the TWG process has reached a point where continuing discussions of the public key issue will yield only marginal results. Simply stated, we believe that over the past 13 months we have explored the technical and national security equity issues to the point where a decision is required on the future direction of digital signature standards.

(b) (5)



~~SECRET~~

~~SECRET~~

(b)(1)
(b)(3)xx
(b)(5)

(S)

[REDACTED]

[REDACTED]

[REDACTED]

(b)(5)

Attachment

APPROVED _____

DISAPPROVED: _____

~~SECRET~~



63

December 26, 1990

MEMORANDUM FOR THE RECORD

SUBJECT: Twenty First Meeting of the NIST/NSA
Technical Working Group (TWG)

The twenty first meeting of the NIST/NSA TWG was held today at the NSA Building, Fort Meade, MD. The TWG members participating in the meeting included:

NIST
Dennis Branstad
Lynn McNulty

NSA
[REDACTED]

Other participants included:

NIST
Ray Kammer

NSA
[REDACTED]

N.R.

Ray Kammer introduced the technical and administrative comparison of the three candidate Public Key Signature Algorithms (aka Digital Signature Algorithms) before the TWG. He stated that NIST staff had prepared the comparison at his request to compare various aspects of the candidates and present the best case for a recommended one. A notebook that does this had been prepared by NIST TWG members and staff and has been given to the NSA TWG members for comment. [REDACTED] acknowledged receipt of the notebook and stated that NSA TWG members will be preparing comments for presentation at the next TWG. They will also provide both an unclassified and a classified statement supporting their preferred candidate algorithm.

Significant discussion was held on the patent issue surrounding public key. RSA/PKP has stated that they would grant non-exclusive, reasonable royalty licenses under its RSA patents if RSA became a standard for digital signatures. Jim Bidzos, President of RSA and PKP, has verbally stated they they would not grant similar licenses under their other patents which they state cover the El Gamal family of signature techniques. [REDACTED] stated that he believed that this family of techniques was developed with support of the government which requires that non-exclusive, reasonable royalty licenses be also granted for them. The issue of what industry considers reasonable royalties was discussed. A proposal for holding a public workshop on the patent issue was made. The patent attorneys of NIST and NSA will be requested to look into this issue by Mr. Kammer and [REDACTED].

(NOTE: Subsequent to the meeting, Dennis Branstad and [REDACTED] confirmed that there was a statement in each of the four patents held by PKP stating that the government has rights under the patents. The specific rights are not stated in the patents.)

The next meeting of the TWG is scheduled for January 8, 1991.

Prepared by:

Dennis K. Branstad
Dennis K. Branstad

Concurrence:

F. Lynn McNulty
F. Lynn McNulty

cc: J. Lyons
R. Kammer
J. Burrows
S. Katzke
M. Smid

4 page attachment - N.R.



NIST

66
UNITED STATES DEPARTMENT OF COMMERCE
National Institute of Standards and Technology
Gaithersburg, Maryland 20899

MEMORANDUM FOR THE RECORD

SUBJECT: Twenty-second Meeting of the NIST/NSA
Technical Working Group (TWG)

(b)(3)* On January 17, 1991, the twenty-second meeting of the NIST/NSA TWG was held at the NSA Building, Fort Meade, MD. The participants in the meeting included:

NIST
Dennis Branstad
Lynn McNulty
Edward Roback

NSA
[REDACTED]

N.R

N.R.

[REDACTED]

Public Key Cryptography Patents. Mr. McNulty advised NSA that NIST has scheduled a meeting of experts on February 5 concerning the legal issues related to the possible adoption by the government of patented public key technology. OK

NEW BUSINESS

N.R.

[REDACTED]

TWG ISSUE #1 - Digital Signature Standard. The NSA representatives began the discussion of this matter by delivering a critique of the Public Key Issue document provided to NSA on December 13, 1990. After several minutes of discussing the assumptions underlying the document, Dr. Branstad asked [REDACTED] if this issue was any longer a technical one. All parties at the meeting agreed that it was not, and it was decided that there would be no further discussion of a proposed public key, digital signature standard by the TWG unless new developments required additional action. This discussion effectively completed TWG Action on Issue #1. OK

(b)(3)*

N.R.

N.R.

Mr. Kammer also introduced Issue #5 (Attachment 1), in which NIST asked NSA to consider whether DSA1, if approved as a Federal Information Processing Standard, would also be approved by NSA for classified use. He saw this as a good selling point which would also emphasize the ability of NIST and NSA to work closely together. A common solution would have economy of scale benefits for the entire government. [REDACTED] inquired if NIST wanted this for SECRET and below, or Type II, or Type I. Mr. Kammer replied that that would be entirely up to NSA but that a commonly agreeable standard could be very useful.

Mr. Kammer asked the TWG to look into ways to promote the use of DSA1. For example, it would be useful to have agreed upon answers to expected questions, so that NIST and NSA could present a common front. One idea proposed was for the government to give preference to digitally-signed software in procurements.

N.R.

Attachments

Attachment 1 - Issue #5

Attachment 2 - Issue #6

Prepared by: Edward Roback

Concurrence: Lynn McNulty
Miles Smid

cc: Ray Kammer



NIST

~~SECRET~~

UNITED STATES DEPARTMENT OF COMMERCE
National Institute of Standards and Technology
Gaithersburg, Maryland 20899

70

MAR 18 1991.

MEMORANDUM FOR THE RECORD

SUBJECT: Twenty-third Meeting of the NIST/NSA
Technical Working Group (TWG)

(4) On March 11, 1991, the twenty-third meeting of the NIST/NSA TWG was held at the NSA Building, Fort Meade, MD. The participants in the meeting included:

(b)(3)*

NIST

NSA

Lynn McNulty
Edward Roback

ISSUE #1 DIGITAL SIGNATURE STANDARD

(5)

Signature

N.R. Mr. McNulty began the meeting with a review of activities concerning Issue #1 since the last TWG meeting. He summarized the results of the two meetings at the Office of Management and Budget (OMB) where Mr. Kammer and [REDACTED] discussed the progress of the NIST/NSA activities with OMB officials regarding a digital signature standard [REDACTED]. He also reviewed information he had received about other senior level meetings and briefings on the signature standard.

(b)(3)*

[REDACTED] contributed his perspective on developments since the last meeting. He asked if the NIST TWG members had seen a copy of a recent letter sent from the Director of NSA to the Director of NIST regarding the digital signature issue. The NIST attendees responded in the negative to this question. The public policy issues inherent in S. 266, "The Counterterrorism Act of 1991" and its relation to the digital signature standard [REDACTED].

N.R.

(b)(3)*

A discussion of the patent issues regarding a proposed digital signature followed. It was agreed by both parties that it would be appropriate to hold another meeting of legal experts within the next few weeks. [REDACTED] asked the NIST participants if we had considered filing for a patent on the DSA #1 algorithm and then allow the courts to settle the various questions issues involved in this matter. Mr. McNulty responded that NIST had not considered this approach, and that NIST was not looking to delay the signature standard any longer by engaging in a prolonged legal battle. NIST accepted the action to hold a second meeting of the patent legal experts to determine what insights have been gained since the first meeting. (NIST Action Item 23-1)

~~SECRET~~

~~SECRET~~

Mr. McNulty concluded the discussion of this aspect of the signature standard by stating that he had been advised that NIST management has accepted NSA's proposal (DSA #1) as the basis for a draft digital signature standard to be published in the Federal Register once the patent issues have been resolved. NIST is currently working on a draft standard that will incorporate the DSA #1 algorithm. This will be provided to NSA review before publication. NSA advised NIST that several typographical errors had been identified in the copy of the DSA #1 document. A corrected copy will be transmitted to NIST.

(b)(5):

Remainder of this page
and next page

~~SECRET~~



NIST

UNITED STATES DEPARTMENT OF COMMERCE
National Institute of Standards and Technology
Gaithersburg, Maryland 20899

APR 24 1991

MEMORANDUM FOR THE RECORD

SUBJECT: Twenty-fifth Meeting of the NIST/NSA
Technical Working Group (TWG)

(b)(3)* On April 19, 1991 the twenty-fifth meeting of the NIST/NSA TWG was held at the Building of the National Security Agency at Ft. Meade, Maryland from 10:00 a.m. to 2:00 p.m. The participants in the meeting included:

NIST

Lynn McNulty
Miles Smid
Ed Roback
Dennis Branstad

NSA

Digital Signature Standard

Mr. Smid provided the members a draft of the Federal Information Processing Standard for the Digital Signature Standard, incorporating the Digital Signature Algorithm, as is the current NIST nomenclature. (See Attachment #1.) NIST requested comments from NSA on the standard by the next TWG meeting. (ACTION - NSA) A brief review of the standard quickly moved to the patent and export issues. NIST agreed to provide an example for the FIPS to NSA for their review. (ACTION - NIST) NSA agreed to provide NIST with unclassified justifications for the selection of DSA1. (ACTION - NSA)

(b)(3)* Background: On April 5, 1991, [redacted] (Assistant to the General Counsel for Research, Technology, and Communications at NSA) provided an initial draft of infringement studies being conducted at NSA related to DSA1 and the claims of four U.S. patents. (See Attachment #2.) [redacted]

(b)(5) [redacted] While NSA was conducting these studies, the Department of Commerce's [redacted] (b)(6)

(b)(7)(C) [REDACTED]
[REDACTED]
[REDACTED] NIST and NSA agreed to look more closely at the patent (a copy of which was provided by NIST to NSA; see Attachment #3).
(b)(7)(C) [REDACTED]
[REDACTED]

(b)(7)(C) In reviewing the export section of the draft FIPS, [REDACTED] agreed to provide NIST with recommended wording for the section. (ACTION [REDACTED]) (Note: the recommended changes were received a few days later; see Attachment #4.) - NSA believes that manufacturers will still have to get an export license - but it will not be on a case by case basis. A single license would be good for all but a very limited group of countries.

In these discussions, NSA requested copies of a recently issued NIST Special Publication (Number 800-002) on public key cryptography authored by James Nechvatal. The document is currently at the printer. (ACTION - NIST)

In discussions regarding alternatives for a hashing algorithm, it was agreed that it was reasonable to say that one is expected within six months.

NR

**NIST**

UNITED STATES DEPARTMENT OF COMMERCE
National Institute of Standards and Technology
Gaithersburg, Maryland 20899

74

MAY 23 1991

MEMORANDUM FOR THE RECORD

SUBJECT: Twenty-seventh Meeting of the NIST/NSA
Technical Working Group (TWG)

On May 23, 1991 the twenty-seventh meeting of the NIST/NSA TWG was held at the [redacted] Building of the National Security Agency at Ft. Meade, Maryland from 9:00 a.m. to 12:00 noon. The participants in the meeting included:

NIST

Lynn McNulty
Miles Smid
Ed Roback

NSA

[redacted]

Digital Signature Algorithm - Technical Issues

[redacted] opened the meeting by announcing that NSA was still working on their comments on the example of the implementation of DSA. Comments would be provided to NIST shortly.

Next, Mr. Smid reviewed the timing figures he obtained for signature and verification using both the DSA and RSA techniques. Using DSA, signing took .27 seconds while verification took 13.95 seconds. The figures, respectively, for RSA were 7.2 and 1.2 seconds. These figures were obtained using a Sun III workstation. NSA indicated that the differences were similar in magnitude to those they had obtained. Mr. Smid also provided NSA with an e-mail message which described a reported break in a two-pass version of MD4 (Attachment #1). Mr. Smid indicated his desire to change the nomenclature in the standard to that more consistent with common usage [e.g., (x,y) to (k1, k2)]. The TWG members interposed no objections.

Also, NIST is preparing a white paper which will examine the supporting infrastructure necessary for the government to effectively implement DSS.

Processing of the Digital Signature Standard

In discussions which followed regarding the announcement of the DSS, four possible critical path items were identified:

1) patent issues;

(b)(3)*

[redacted] indicated that [redacted] NSA's Patent Counsel, had completed the patent infringement study of the four PKP patents and the Schnorr patent. [redacted]

(b)(5)

[redacted] indicated that the report had been sent to the Department of Commerce Patent Counsel (Attachment #2). NSA clearly indicated that the burden of the final decision was with NIST although they were available for technical consultations.

Mr. McNulty also indicated that had heard informally that IBM was independently examining the Schnorr patent and may render an opinion as to its validity. On a related matter, it was mentioned that AT&T had discussed an El Gamal-based public-key technique with Dr. Schnorr and obtained his assurances that AT&T's technique did not infringe upon his patent.

2) Secretarial-level briefing;

As discussions progressed, it became clear that this item was not going to be a hinderance as Mr. Kammer has obtained the Secretary of Commerce's approval to proceed with the announcement of the draft digital signature standard.

3) Obtaining NSA's formal comments on the draft Federal Register notice and draft DSS; and

It was agreed that once NSA's comments on the DSA implementation example were received by NIST, NIST would prepare a final version of the standard to be submitted to NSA for final comment. (ACTION - NIST)

4) Obtaining an NSA answer to Warner/classified applicability of the DSA.

(b)(3)*

[redacted] indicated that it appeared as though NSA would agree that the DSA could be used for Warner and classified applications. A formal decision from the agency would be forthcoming. However, it was noted that some of the support mechanisms/implementation infrastructure may be different. Since FIPS do not generally apply to classified systems, it was agreed that NSA would provide approved wording for inclusion in the FIPS applicability section (e.g., to the effect that "NSA has informed NIST that..."). Implementation for the classified community may require action through the NSD-42 committee structure.



NIST

UNITED STATES DEPARTMENT OF COMMERCE
National Institute of Standards and Technology
Gaithersburg, Maryland 20899

75

June 19, 1991

MEMORANDUM FOR THE RECORD

From: Lynn McNulty, Associate Director for Computer Security

Subject: Summary of Decisions Made at Meeting Regarding the
Digital Signature Standard

(b)(3)* On 0930 hours on June 6 the undersigned met with Mr. Ray Kammer, Mr. James Burrows and [REDACTED] (NSA) to discuss the progress made to date regarding the digital signature standard. The meeting, held in Mr. Kammer's office, began with a review of the present status of the project. This review focused upon an options paper presented by Mr. Burrows. A copy of this document is attached.

Following this discussion the following decision were made:

(b)(5)

[REDACTED]

(b)(3)*

o The El Gamal algorithm was now the preferred choice. [REDACTED] stated that NSA has been reviewing of El Gamal and may have found a way to improve its efficiency without degrading the security of the base algorithm. The algorithm to be used as the basis for the standard will be a variant of El Gamal.

As a result of the decision to select El Gamal the following responsibilities were accepted by NIST and NSA.

NSA:

1. Obtain written opinion from patent attorney on whether the El Gamal variant to be adopted as the base algorithm for the standard infringes the Diffie-Hellman patent held by Public Key Partners.

2. Complete technical evaluation of the El Gamal variant and provide NIST with results at the TWG meeting of June 13.

NIST:

1. Prepare draft FIPs document based upon El Gamal as the base algorithm and present to NSA at TWG meeting.

2. Request DOC patent attorney to review El Gamal from the infringement perspective and prepare written opinion.

Attachment



NIST

UNITED STATES DEPARTMENT OF COMMERCE
National Institute of Standards and Technology
Gaithersburg, Maryland 20899

76

JUL 17 1991

MEMORANDUM FOR THE RECORD

SUBJECT: Twenty-eighth Meeting of the NIST/NSA
Technical Working Group (TWG)

On June 14, 1991 the twenty-eighth meeting of the NIST/NSA TWG was held at the Building of the National Security Agency at Ft. Meade, Maryland from 9:00 a.m. to 11:30 a.m. The participants in the meeting included:

NIST

Lynn McNulty
Miles Smid
Ed Roback

NSA



opened the meeting without a set agenda by noting that things were moving very fast. A meeting has been set up with and Mr. Kammer at NIST on Thursday, June 20, 1991 at which it is anticipated the final deliberations regarding the two algorithms will occur.

Mr. McNulty relayed that during consultations with OMB, they advised that there not be a direct USG approach to . It was also noted that there simply was not enough time to process the standard in time for the June hearings. indicated that it should be the role of the TWG to review the pending technical issues so that management could be fully informed for the meeting on June 20. At this point, the NSA-prepared "Technical Pending Digital Signature" paper was reviewed. (Attachment #1) NSA informed NIST that the decision memorandum on the applicability of the signature technique to Warner and classified applications was being prepared for Dr. Hearn.

In technical discussions which followed, NSA provided timings for the El Gamal variant (DSA4) and Schnorr variant (DSA1). (Attachment #2) Mr. Smid indicated that he would like to receive both implementations in magnetic form for analysis. (ACTION - NSA) Regarding the implementation of a third simulation, it was agreed that NIST's implementation would serve this function.

prepared for submission to



NIST

UNITED STATES DEPARTMENT OF COMMERCE
National Institute of Standards and Technology
Gaithersburg, Maryland 20899
OFFICE OF THE DIRECTOR

JUL 31 1991

80



MEMORANDUM FOR Admiral William O. Studeman
Director
National Security Agency

From: John W. Lyons *John W. Lyons*
Director
National Institute of Standards and Technology

Subject: Draft Digital Signature Standard and
Federal Register Notice

Attached for your review is the final draft of the Digital Signature Standard which we plan to propose as a Federal Information Processing Standard (FIPS). This draft FIPS incorporates the Digital Signature Algorithm developed through the joint NSA/NIST Technical Working Group process. I have also attached the draft Federal Register notice announcing the standard for public comment.

I would appreciate receiving NSA's final comments on this document. Once we have received them, I plan to move expeditiously to initiate the formal clearance process.

Thank you for your attention to this request.

Attachments

*Attachment: Draft FIPS Pub.
19 pages withheld (b)(5)*



~~CONFIDENTIAL~~

NATIONAL SECURITY AGENCY
CENTRAL SECURITY SERVICE
FORT GEORGE G. MEADE, MARYLAND 20755-6000



6 AUG 1991

Dr. John W. Lyons
Director of National Institute
of Standards and Technology
Gaithersburg, Maryland 20899

Dear Dr. Lyons:

(U) Please reference your memorandum of 31 July 1991. We have reviewed the draft Digital Signature Standard (DSS) and related Federal Register notice you provided with your memorandum. We have no comment on these drafts.

(C) The DSS reflected in the enclosure to your memorandum, a variant of the El Gamal algorithm, is compatible with the concerns I expressed to you in my letter of 15 February 1991. I am pleased our mathematicians were able to develop this digital signature algorithm to satisfy critical user performance requirements. [REDACTED]

(U) The DSS marks a major milestone in our cooperation in furtherance of NIST's implementation of the Computer Security Act of 1987 (Act). Such cooperation will serve both agencies well as we continue to advance the purposes of the Act in the months and years ahead.

Very respectfully,

W. O. Studeman

W. O. STUDEMAN
Vice Admiral, U.S. Navy
Director

Copy Furnished:
DIR, FBI



UNITED STATES DEPARTMENT OF COMMERCE
National Institute of Standards and Technology
Gaithersburg, Maryland 20899

National Computer Systems Laboratory

Dec. 22, 1989

MEMORANDUM FOR: Lynn McNulty

FROM: Roy Saltman *RS*

SUBJECT: Public Key Encryption (PKE) Algorithms in Wide Use

At your request, I have obtained an extensive bibliography of unclassified references, have reviewed some of this literature, and have spoken with a number of knowledgeable individuals about the current publicly-acknowledged use of PKE in North America and Western Europe.

PKE is a cryptosystem in which each communicator has a pair of data keys, one of which is public (i.e., known to communication partners) while the other is private. A message may be encoded with either of the keys but must be decoded with the other. In a PKE system acceptable for widespread use, breaking the system, i.e., discovering the private key from knowledge of the public key, must be "computationally infeasible." This implies that the resources required would be far beyond that available to almost all organizations.

The RSA Algorithm

It seems clear that the RSA algorithm is widely known and widely used. In the US, the patent on products using the RSA algorithm is held by RSA Data Security, Inc. of Redwood City, CA. The name RSA is formed from the initials of the three MIT professors who invented the algorithm and formed the company. The inventors are Ronald Rivest, Adi Shamir, and Leonard Adleman [1]. There is no RSA patent in Europe.

The RSA system makes use of the fact that factoring the arithmetic product of two large prime numbers appears to be "computationally infeasible." [2] For RSA data encryption, the message is encrypted with the receiver's public number; it is decrypted with the receiver's private number. For the purpose of digital signature, the message is encrypted with the sender's private number; it is decrypted with the sender's public number.

Thus, RSA is a most versatile public-key cryptosystem. It supports both secrecy and authentication, and can provide complete and self-contained support for public key distribution and signatures.

CCITT Recommendation X.509-1988, entitled The Directory - Authentication Framework, defines a framework for the provision of authentication services by the Directory. Information held by the Directory, collectively known as the Directory Information

Base, is typically used to facilitate communication among objects such as open system interconnection (OSI) application-entities, people, terminals, and distribution lists. The authentication system described in X.509-1988 assumes the use of PKE, and Annex B of that document is entitled An Introduction to Public Key Cryptography. Annex C of X.509-1988 (not officially part of the standard) is entitled The RSA Public Key Cryptosystem, and the RSA system is described therein. Thus, it appears that the RSA algorithm is sufficiently widely known and accepted to be used as a normative example in an important international standard.

On the European continent, an organization called TeleTrust has been formed to institutionalize the interchange of electronic messages. Countries in which Teletrust operates include Finland, France, Germany, Italy, Netherlands, and Sweden. The national organizations have relationships with banks and the national PTTs. The RSA algorithm "plays a central role within Teletrust," according to Teletrust literature, in providing for electronic signatures.

In the UK, EftPos UK has been established by the Association for Payment Clearing Services, an organization that, from its name, appears to serve a similar function to that served by the National Automated Clearing House Association in the US. "The RSA encryption standard (has been) chosen by EftPos UK" and "Plessey Crypto has designed a low cost chip (for RSA operation) able to provide the level of security demanded by banks," according to a UK financial industry newsletter.

Also in the UK, a company named Sophos Ltd. is producing encryption software using the RSA algorithm (and other algorithms, see below). This company also sells in Scandinavia, the Low Countries, Greece and Cyprus, Ireland, Italy, Israel, Australia and New Zealand, and Singapore. The company claims to be "the leading British company to specialize in data security."

In the US, Internet, a computer network that ties together hundreds of academic, government, and corporate computers, has adopted RSA for key management. As noted in its draft publication RFC 1114, "the RSA cryptographic algorithm.....has been selected for use in this key management system." RFC 1114 also notes that "the key management architecture described in this RFC is compatible with the authentication framework described in X.509."

In addition, RSA Data Security and the Digital Equipment Corporation have signed an agreement under which Digital obtains access to the same technology that Internet proposes to use. Digital officials have stated that they expect to integrate RSA technology into a broad array of software and hardware products. [3] Corporate uses of RSA products are growing also. PC Week has reported that Citicorp is using RSA Data Security's Mailsafe software in its Citimail internal E-mail service for the bank and its international subsidiaries. [4]

Implementations of the RSA algorithm in the USA are being done by RSA Data Security and CYLINK. The latter has a key management processor chip that can handle moduli of up to 1024 bits; operations of modular addition, multiplication, and exponentiation are supported.

Diffie-Hellman Key Exchange

The first public key exchange technique proposed in the open literature was due to Diffie and Hellman [5], and is referred to here as DH. Although not exactly an asymmetric key encryption technique, DH has the property of allowing two people to share a secret key by exchanging only non-secret numbers over an insecure communications link. It may be used to support DES encryption by supplying two communicating parties with the necessary data to create a jointly used DES data key without the help of a central key distribution center. Thus, DES key management is significantly simplified.

DH does not require the search for two strong primes, as is required by RSA. The cryptographic security of DH depends on the computational infeasibility of computing a discrete logarithm to re-obtain a previously exponentiated value. Some experts believe that the difficulty of this operation is equal to that of determining the factors required for the solution of the RSA system, while other experts believe that the difficulty of solving the discrete logarithm problem is actually greater.

When using DH, all communicators in the network have the same two non-secret constants: a single large prime number, and a positive integer less than the prime. Then, two prospective communicators each select a single private random integer X , and each applies it to a particular exponentiation formula involving the two network constants. The result of the exponentiation is a public number Y for each communicator. The communicators then exchange their public numbers. Each then makes an additional computation (forming parameter Z) by combining their respective secret numbers with the received public number, using a particular exponentiation formula. The computations are such that each communicator will generate exactly the same value of parameter Z . Then, part of this shared secret number Z can be used as a common DES data encryption key.

An important feature of DH is the fact that the shared secret number Z depends on the random secret numbers that the two communicators independently selected. Thus, both communicators must participate in the calculation of Z ; one alone cannot control the common data key.

The British company, Sophos, identified above, sells a "public key system for digital signature and encryption of communications." This product uses "512 bit RSA or Modified Diffie Hellman (MDH) encryption of a DES key, followed by DES encryption of

data using Cipher Block Chaining." The MDH algorithm used by Sophos may be similar to DH, or to the closely related El Gamal procedure, or it may be similar to the DH variation called Pohlig-Hellman (see below).

DH key exchange is implemented in software by CYLINK in the form of their SEEK algorithm, using the processor chip mentioned above under RSA.

El Gamal Digital Signature

The signature scheme was invented by T. El Gamal [6], a student of Hellman. The scheme is based, similarly to DH, on the difficulty of inverting an exponentiation by taking a discrete logarithm. To use the system, a signer selects a private number X and by exponentiation creates a public number Y , exactly as is done in the DH process. Then, for each message, the signer selects an additional message-specific private number R and by a similar exponentiation process, creates a message-specific public number V . The signer also creates a hash value of the message to be sent, according to a formula that the message recipient may also use. The signer also creates a public number S by a combination of the networkwide private number X , the message-specific private number R , the message-specific public number V , and the hash value. Knowing S does not give enough information to determine the private numbers R or X .

The message is transmitted, along with the message-specific public numbers V and S . The recipient already knows the sender's networkwide public number Y . The recipient can recompute the hash value from the message and use it in an exponentiation formula involving V and Y . If the recipient's hash value is the same as the sender's hash value, the exponentiation formula will equal an exponentiation of the signer's value S . This equivalence will demonstrate that the message must have originated with the actual sender.

The El Gamal digital signature scheme is being implemented by Newbridge Microsystems (formerly Calmos) of Kanata, Ontario, Canada.

Pohlig-Hellman Variation

As in DH, the sender and receiver each select private networkwide numbers X and compute from them public networkwide numbers Y . In Pohlig-Hellman, the sender also selects a message-specific private random number R and computes from it, by exponentiation, a message-specific public number V . A secret encryption key Z is also computed by the sender from the receiver's networkwide public number Y and the sender's message-specific private number R . The encrypted message is transmitted, but the encryption key is not transmitted.

However, the receiver can re-create the encryption key Z using

the sender's message-specific public number V and the receiver's networkwide private number X . In addition, the receiver can generate the necessary decryption key from Z using the Euler totient function [7]. Then, the receiver can decrypt the message. Note that the encryption and decryption keys are message-specific.

CYLINK implements encryption via Pohlig/Hellman, but it is not efficient compared to DES.

Other Algorithms

The concepts presented above are those that are generally publicly known, and are reasonably secure. Diffie [2] mentions knapsack systems, which he states have been broken. However, J. Nechvatal of NIST has stated that the Chor/Rivest variation of the knapsack scheme [8] still survives. Key generation with the latter scheme may take several hours, but encryption is faster than with RSA. Diffie [2] also has discussed a system invented by R. McEliece. Diffie states that:

"McEliece's system has never achieved wide acceptance and has probably never even been considered for implementation in any real application. This may be because the public keys are quite large, requiring on the order of a million bits; it may be because the system entails substantial expansion of the data; or it may be because McEliece's system bears a frightening structural similarity to the knapsack systems..."

Work on the basic McEliece concept is continuing.

There are other schemes that are based on the so-called "word problem," but there is no evidence of implementation. There may be other types of systems in use, but these, if any, do not appear in the unclassified literature. Recently, I had the opportunity to meet Fernand Simon, Director of Research for SWIFT (Society for Worldwide Interbank Financial Transfers), headquartered in Brussels. Simon indicated that SWIFT would be using PKE but refused to state which algorithm. He implied that SWIFT had its own private algorithm.

References

- [1] R. Rivest, A. Shamir, and L. Adleman, "A Method For Obtaining Digital Signatures and Public-Key Cryptosystems," Communications of the ACM, vol. 21, February 1978, pp. 120-126.
- [2] Whitfield Diffie, "The First Ten Years of Public-Key Cryptography," Proceedings of the IEEE, vol. 76, no. 5, May 1988.
- [3] New York Times, "Data Network to Use Code to Insure Privacy," by Vin McLellan, March 21, 1989.
- [4] PC Week, "Citicorp Takes the Lead in Addressing E-Mail Security," by Matt Kramer, vol. 5, no. 35, August 29, 1988.
- [5] W. Diffie and M. E. Hellman, "New Directions in Cryptography," IEEE Transactions on Information Theory, vol. IT-22, November 1976, pp. 644-654.
- [6] T. El Gamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," IEEE Transactions on Information Theory, vol. IT-31, July 1985, pp. 469-472.
- [7] S. C. Pohlig and M. E. Hellman, "An improved algorithm for computing logarithms over $GF(p)$ and its cryptographic significance," IEEE Transactions on Information Theory, vol. IT-24, January 1978, pp. 106-110.
- [8] B.Z. Chor, Two Issues in Public Key Cryptography: RSA Bit Security and a New Knapsack Type System, Cambridge, MA: MIT Press, 1986.

STATEMENT OF
RAYMOND G. KAMMER
ACTING DIRECTOR, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
BEFORE THE
SUBCOMMITTEE ON TELECOMMUNICATIONS AND FINANCE
COMMITTEE ON ENERGY AND COMMERCE

APRIL 29, 1993

Mr. Chairman and Members of the Subcommittee:

Good morning. Thank you for inviting me to testify. I am Raymond G. Kammer, Acting Director of the National Institute of Standards and Technology of the U.S. Department of Commerce. Under the Computer Security Act of 1987, NIST is responsible for the development of standards for protecting unclassified government computer systems, except those commonly known as Warner Amendment systems (as defined in Title 10 USC 2315).

NIST has a long-established program of developing computer security guidelines and standards for federal agencies. Many of these are also used, on a voluntary basis, by the private sector. We have published guidance on computer security training and awareness, identification and authentication, open systems security, incident response, cryptographic standards, trusted systems, and many other facets of computer security.

Today, however, I plan to address the following topics which I believe are most directly germane to your invitation:

- * The need for good information security technology to protect computer and telecommunications systems and networks;
- * NIST's activities in telecommunications switch security;
- * the planned recertification of the Data Encryption Standard;
- * NIST's proposed Digital Signature Standard;
- * the recent White House announcement of a new encryption technology, called the Clipper Chip; and
- * the President's directive to review advanced telecommunications and encryption technology.

Need for Computer Security

Strong security technology is required in modern communications systems and networks to protect sensitive and valuable information. Government agencies and private corporations depend upon the integrity and availability of their communications system in order to do business. Computer viruses, network worms, hackers, and other threats against our systems emphasize the importance of telecommunications security.

Additionally, I have grown convinced, through strong anecdotal evidence, most of it shared on a proprietary basis, of the growing threat to American business from "economic espionage." Much has been reported in the press of the activities of foreign intelligence services targeting American firms, and sharing their findings with competing foreign firms. I am convinced that American firms need strong security, and in particular, strong cryptography, to protect against such threats.

More importantly, the Administration is committed to working with the private sector to spur the development of a National Information Infrastructure which will use new telecommunications and computer technologies to give Americans unprecedented access to information. This infrastructure of high-speed networks ("information superhighways") will transmit video, images, HDTV programming, and huge data files as easily as today's telephone system transmits voice. Appropriate security techniques may at times be integrated into such systems.

Telecommunications Security

Federal telephone and computer networks depend upon reliable and secure telecommunications capabilities, both of long-distance carriers and local private-branch exchanges (PBXs). To examine security issues of telecommunications networks, including issues of PBX security and telecommunications switch security, NIST is currently setting up a Telecommunications Security Analysis Center. This Center will expand on initial research we have conducted on the vulnerability of telecommunications switches.

Telecommunications switches are an integral part of the security of the public switched network. Security problems in switches can result in serious problems such as toll fraud, unauthorized and illegal eavesdropping, or the disabling of switches, which would result in bringing down part of the public switched network.

NIST has been monitoring the growth of switch-related abuse and has been analyzing switches to be able to address the types of crimes that could be perpetrated in the future. This work includes studying the growing ease of perpetrating these crimes. There are several areas of concern:

- * Toll fraud. Current research indicates that the problem is well over \$1 billion per year. While not all toll-fraud is accomplished technically, telecommunications switches are vulnerable to hackers who can gain unauthorized access to the use of long-distance services. This is a particular vulnerability to the owners of PBXs, who can lose considerable sums if their systems are inadequately protected. Good system configuration control is one good security measure we are examining.

- * Network Availability. There have been no cases of intruders purposefully bringing down parts of the public switched network. The President's National Security Telecommunications Advisory Committee (NSTAC) concluded that "Until there is confidence that strong comprehensive computer security programs are in place, the industry should assume that a motivated and resourceful adversary in one concerted manipulation of the network software could degrade at least portions of the PSN."
- * Unauthorized Eavesdropping. If unauthorized access is gained to telecommunications switches, which is really just a computer that switches phone calls, a hacker can gain access to the contents of phone conversations and other information transmitted through a switch. This unauthorized eavesdropping can be either "real-time," as the conversations occur, or the intruders can arrange to have the conversations and data electronically transmitted to another telecommunications switch or computer for later analysis.

The purpose of the Telecommunications Security Analysis Center will be to:

- * Develop tools and techniques to analyze very complex systems such as switches;
- * Provide informal security guidance and advice to federal agencies on procurement of telecommunications switches;
- * Perform security analyses of commercial switches in both laboratory and real world environments; and
- * Develop standards and guidance for use in securing switches and in building more secure switches, while providing for the legitimate needs of law enforcement, under proper court order, to protect the American public.

As we pursue this research, we will be pleased to provide additional information on our findings to the Committee.

The Data Encryption Standard

The current government standard for the encryption of data is known as the Data Encryption Standard (DES), which was first approved as a Federal Information Processing Standard in 1977. DES is widely used within both the government and the private sector for the protection of sensitive information, including financial information, medical information, and Privacy Act data. DES represents a proven twenty year old technology with DES products available in the marketplace for the last 15 years.

Last year, NIST formally solicited comments on the recertification of DES. After reviewing those comments, and the other technical inputs that I have received, I plan to recommend to the Secretary of Commerce that he recertify DES for another five years. I also plan to suggest to the Secretary that when we announce the recertification we state our intention to consider alternatives to it over the next five years. By putting that announcement on the table, we hope to give people an opportunity to comment on orderly technological transitions. In the meantime, we need to consider the large installed base of systems that rely upon this proven standard.

NIST's Proposed Digital Signature Standard

The majority of the cryptographic-based security requirements in computer and network systems involve the need for strong identification and authentication. One method which we believe holds a capacity for significant improvements in security and also cost-savings by automating paper processes is the use of digital signatures.

A digital signature is a computer-based method of "sealing" an electronic message in such a way that its contents cannot be changed or forged without detection and that the identity of the originator of the communication can be verified. The digital signature for a message is simply a code, or large number, that is unique for each message and each message originator (within a very high, known probability). A digital signature is computed for a message by computing a representation of the message (called a "hash" code) and a cryptographic process that uses a key associated with the message originator. Any party with access to the public key, message, and signature can verify the signature. If the signature verifies correctly, the receiver (or any other party) has confidence that the message was signed by the owner of the public key and the message has not been altered after it was signed.

In 1991, NIST proposed a draft Digital Signature Standard (DSS). We received about 130 public comments. We have been reviewing these comments and revising the standard as appropriate to respond to those comments. Additionally, we have examined and are currently dealing with two claims of patent infringement, which we believe will be successfully resolved in the not-too-distant future. Once this occurs, the Secretary of Commerce needs to decide to approve the DSS as a Federal Information Processing Standard. It will then complement the Secure Hash Standard which was recently approved by the Secretary of Commerce as Federal Information Processing Standard 180.

We anticipate that the DSS will find many uses within government computer systems and networks. For example, DSS could be employed in electronic funds transfer systems. Suppose an electronic funds transfer message is generated to request that \$100.00 be transferred from one account to another. If the message was passed over an unprotected network, it may be possible for an adversary to alter the message and request a transfer of \$1000.00. Without additional information, it would be difficult, if not impossible, for the receiver to know the message had been altered. However if the DSS was used to sign the message before it was sent, the receiver would know the message had been altered because it would not verify correctly. The transfer request could then be denied.

DSS could be employed in a variety of business applications requiring a replacement of handwritten signatures. One example is Electronic Data Interchange (EDI). EDI is the computer-to-computer interchange of messages representing business documents. In the federal government, this technology is being used to procure goods and services. Digital signatures could be used to replace handwritten signatures in these EDI transactions. For instance, contracts

between the government and its vendors could be negotiated electronically. A government procurement official could post an electronically signed message requesting bids for office supplies. Vendors wishing to respond to the request may first verify the message before they respond. This assures that the contents of the message have not been altered and that the request was signed by a legitimate procurement official. After verifying the bid request, the vendor could generate and sign an electronic bid. Upon receiving the bid, the procurement official could verify that the vendor's bid was not altered after it was signed. If the bid is accepted, the electronic message could be passed to a contracting office to negotiate the final terms of the contract. The final contract could be digitally signed by both the contracting office and the vendor. If a dispute arose at some later time, the contents of contract and the associated signatures could be verified by a third party.

DSS is also likely to find widespread applications in the health care field. It might be used to sign digital images, for example, to assure that they remain safe against unauthorized modifications.

DSS could also be useful in the distribution of software. A digital signature could be applied to software after it has been validated and approved for distribution. Before installing the software on a computer, the signature could be verified to be sure no unauthorized changes (such as the addition of a virus) have been made. The digital signature could be verified periodically to ensure the integrity of the software.

In database applications, the integrity of information stored in the database is often essential. DSS could be employed in a variety of database applications to provide integrity. For example, information could be signed when it was entered into the database. To maintain integrity, the system could also require that all updates or modifications to the information be signed. Before signed information was viewed by a user, the signature could be verified. If the signature verified correctly, the user would know the information was not altered by an unauthorized party. The system could also include signatures in the audit information to provide a record of users who modified the information.

The DSS can also be used in conjunction with more secure identification and authentication systems, for the protection of access to both computer and telecommunication systems.

A New Encryption Technology: The Clipper Chip

Approximately two weeks ago, the White House announced our intention, based on a new encryption technology, the Clipper Chip, to initiate a voluntary program to improve the security and privacy of telephone communications while meeting the legitimate needs of law enforcement.

This initiative will involve the creation of new products to accelerate the development and use of advanced and secure telecommunications networks and wireless communications links - the security of the very systems you are examining here today.

Sophisticated encryption technology, including the DES, has been used for years to protect electronic funds transfer. It is now being used to protect electronic mail and computer files. While encryption technology can help Americans protect business secrets and the unauthorized release of personal information, it also can be used by terrorists, drug dealers, and other criminals.

A state-of-the-art microcircuit, the "Clipper Chip," has been developed by government engineers. The chip represents a new approach to encryption technology. It can be used in new,

relatively inexpensive encryption devices that can be attached to an ordinary telephone. It scrambles telephone communications using an encryption algorithm that is more powerful than many in commercial use today. The Clipper algorithm with an 80 bit long cryptographic key is approximately 16 million times stronger than DES. It would take a CRAY YMP over 200 years to solve one DES key. It would take the same machine over a billion years to solve one Clipper Chip key.

This new technology offers opportunities for companies to protect proprietary information, protect the privacy of personal phone conversations and prevent unauthorized release of data transmitted electronically. At the same time this technology preserves the ability of federal, state and local law enforcement agencies to intercept lawfully the phone conversations of criminals.

Protection of confidentiality of information is of critical concern to the nation. So too is the ability of law enforcement to provide safe streets and neighborhoods. Americans demand the very best in law enforcement - at the federal, state and local level. Citizens insist upon a quick response to terrorist threats, organized crime, and drug dealers, while preserving our Constitutional rights. Past experience clearly shows that one critical technology successfully used to prosecute organized crime is the use of court-authorized wiretaps. Unquestionably, these lawful electronic intercepts have saved lives and been critical to bringing criminals to justice. The "Clipper Chip" is also a powerful tool which will be used by law enforcement to protect its own sensitive communications from illicit criminal monitoring.

A "key-escrow" system is envisioned that would ensure that the "Clipper Chip" is used to protect the privacy of law-abiding Americans. Each device containing the chip will have two unique "keys," numbers that will be needed by authorized government agencies to decode messages encoded by the device. When the device is manufactured, the two keys would be deposited separately in two "key-escrow" data bases established by the Attorney General. Access to these keys would be limited to government officials with legal authorization to conduct a wiretap.

The President has asked the Attorney General to make arrangements with appropriate entities who would hold the keys for the key-escrow microcircuits installed in communications equipment. I understand that the Attorney General is currently studying these procedures and options for who will serve as the key escrow holders.

Since the announcement from the White House, I have stressed that the "Clipper Chip" technology provides law enforcement with no new authorities to access the content of the private conversations of Americans. Also, some have claimed that there is a hidden trapdoor in the chip or the algorithm. I cannot state it more simply: no trapdoor exists.

The chip is an important step in addressing the problem of encryption's dual-edge sword: encryption helps to protect the privacy of individuals and industry, but it also can shield criminals and terrorists. We need the "Clipper Chip" and other approaches that can both provide law-abiding citizens with access to the encryption they need and prevent criminals from using it to hide their illegal activities.

Presidential Directive for Advanced Telecommunications and Encryption Review

In order to assess technology trends and explore new approaches and technologies (like the key-escrow system), the President has directed government agencies to develop a comprehensive policy on encryption and advanced telecommunications technology that accommodates:

- * the privacy of our citizens, including the need to employ voice or data encryption for business purposes;
- * the ability of authorized officials to access telephone calls and data, under proper court or other legal order, when necessary to protect our citizens;
- * the effective and timely use of the most modern technology to build the National Information Infrastructure needed to promote economic growth and the competitiveness of American industry in the global marketplace; and
- * the need of U.S. companies to manufacture and export high technology products.

The President has directed early and frequent consultations with affected industries, the Congress and groups that advocate the privacy rights of individuals as policy options are developed.

I anticipate being a member of the governmental review panel which will study this issue.

I will again stress what we have stated previously. Encryption technology will play an increasingly important role in future network infrastructures and the Federal Government must act quickly to develop consistent, comprehensive policies regarding its use. The Administration is committed to policies that protect all Americans' right to privacy while also protecting them from those who break the law.

Thank you Mr. Chairman, I would be pleased to answer any questions.



Clipper

THE WHITE HOUSE

Office of the Press Secretary

For Immediate Release

April 16, 1993

STATEMENT BY THE PRESS SECRETARY

The President today announced a new initiative that will bring the Federal Government together with industry in a voluntary program to improve the security and privacy of telephone communications while meeting the legitimate needs of law enforcement.

The initiative will involve the creation of new products to accelerate the development and use of advanced and secure telecommunications networks and wireless communications links.

For too long there has been little or no dialogue between our private sector and the law enforcement community to resolve the tension between economic vitality and the real challenges of protecting Americans. Rather than use technology to accommodate the sometimes competing interests of economic growth, privacy and law enforcement, previous policies have pitted government against industry and the rights of privacy against law enforcement.

Sophisticated encryption technology has been used for years to protect electronic funds transfer. It is now being used to protect electronic mail and computer files. While encryption technology can help Americans protect business secrets and the unauthorized release of personal information, it also can be used by terrorists, drug dealers, and other criminals.

A state-of-the-art microcircuit called the "Clipper Chip" has been developed by government engineers. The chip represents a new approach to encryption technology. It can be used in new, relatively inexpensive encryption devices that can be attached to an ordinary telephone. It scrambles telephone communications using an encryption algorithm that is more powerful than many in commercial use today.

This new technology will help companies protect proprietary information, protect the privacy of personal phone conversations and prevent unauthorized release of data transmitted electronically. At the same time this technology preserves the ability of federal, state and local law enforcement agencies to intercept lawfully the phone conversations of criminals.

A "key-escrow" system will be established to ensure that the "Clipper Chip" is used to protect the privacy of law-abiding Americans. Each device containing the chip will have two unique

"keys," numbers that will be needed by authorized government agencies to decode messages encoded by the device. When the device is manufactured, the two keys will be deposited separately in two "key-escrow" data bases that will be established by the Attorney General. Access to these keys will be limited to government officials with legal authorization to conduct a wiretap.

The "Clipper Chip" technology provides law enforcement with no new authorities to access the content of the private conversations of Americans.

To demonstrate the effectiveness of this new technology, the Attorney General will soon purchase several thousand of the new devices. In addition, respected experts from outside the government will be offered access to the confidential details of the algorithm to assess its capabilities and publicly report their findings.

The chip is an important step in addressing the problem of encryption's dual-edge sword: encryption helps to protect the privacy of individuals and industry, but it also can shield criminals and terrorists. We need the "Clipper Chip" and other approaches that can both provide law-abiding citizens with access to the encryption they need and prevent criminals from using it to hide their illegal activities. In order to assess technology trends and explore new approaches (like the key-escrow system), the President has directed government agencies to develop a comprehensive policy on encryption that accommodates:

- the privacy of our citizens, including the need to employ voice or data encryption for business purposes;
- the ability of authorized officials to access telephone calls and data, under proper court or other legal order, when necessary to protect our citizens;
- the effective and timely use of the most modern technology to build the National Information Infrastructure needed to promote economic growth and the competitiveness of American industry in the global marketplace; and
- the need of U.S. companies to manufacture and export high technology products.

The President has directed early and frequent consultations with affected industries, the Congress and groups that advocate the privacy rights of individuals as policy options are developed.

The Administration is committed to working with the private sector to spur the development of a National Information Infrastructure which will use new telecommunications and computer technologies to give Americans unprecedented access to information. This infrastructure of high-speed networks ("information superhighways") will transmit video, images, HDTV programming, and huge data files as easily as today's telephone system transmits voice.

Since encryption technology will play an increasingly important role in that infrastructure, the Federal Government must act quickly to develop consistent, comprehensive policies regarding its use. The Administration is committed to policies that protect all Americans' right to privacy while also protecting them from those who break the law.

Further information is provided in an accompanying fact sheet. The provisions of the President's directive to acquire the new encryption technology are also available.

For additional details, call Mat Heyman, National Institute of Standards and Technology, (301) 975-2758.

QUESTIONS AND ANSWERS ABOUT THE CLINTON ADMINISTRATION'S
TELECOMMUNICATIONS INITIATIVE

- Q: Does this approach expand the authority of government agencies to listen in on phone conversations?
- A: No. "Clipper Chip" technology provides law enforcement with no new authorities to access the content of the private conversations of Americans.
- Q: Suppose a law enforcement agency is conducting a wiretap on a drug smuggling ring and intercepts a conversation encrypted using the device. What would they have to do to decipher the message?
- A: They would have to obtain legal authorization, normally a court order, to do the wiretap in the first place. They would then present documentation of this authorization to the two entities responsible for safeguarding the keys and obtain the keys for the device being used by the drug smugglers. The key is split into two parts, which are stored separately in order to ensure the security of the key escrow system.
- Q: Who will run the key-escrow data banks?
- A: The two key-escrow data banks will be run by two independent entities. At this point, the Department of Justice and the Administration have yet to determine which agencies will oversee the key-escrow data banks.
- Q: How strong is the security in the device? How can I be sure how strong the security is?
- A: This system is more secure than many other voice encryption systems readily available today. While the algorithm will remain classified to protect the security of the key escrow system, we are willing to invite an independent panel of cryptography experts to evaluate the algorithm to assure all potential users that there are no unrecognized vulnerabilities.
- Q: Whose decision was it to propose this product?
- A: The National Security Council, the Justice Department, the Commerce Department, and other key agencies were involved in this decision. This approach has been endorsed by the President, the Vice President, and appropriate Cabinet officials.

Q: Who was consulted? The Congress? Industry?

A: We have on-going discussions with Congress and industry on encryption issues, and expect those discussions to intensify as we carry out our review of encryption policy. We have briefed members of Congress and industry leaders on the decisions related to this initiative.

Q: Will the government provide the hardware to manufacturers?

A: The government designed and developed the key access encryption microcircuits, but it is not providing the microcircuits to product manufacturers. Product manufacturers can acquire the microcircuits from the chip manufacturer that produces them.

Q: Who provides the "Clipper Chip"?

A: Mykotronx programs it at their facility in Torrance, California, and will sell the chip to encryption device manufacturers. The programming function could be licensed to other vendors in the future.

Q: How do I buy one of these encryption devices?

A: We expect several manufacturers to consider incorporating the "Clipper Chip" into their devices.

Q: If the Administration were unable to find a technological solution like the one proposed, would the Administration be willing to use legal remedies to restrict access to more powerful encryption devices?

A: This is a fundamental policy question which will be considered during the broad policy review. The key escrow mechanism will provide Americans with an encryption product that is more secure, more convenient, and less expensive than others readily available today, but it is just one piece of what must be the comprehensive approach to encryption technology, which the Administration is developing.

The Administration is not saying, "since encryption threatens the public safety and effective law enforcement, we will prohibit it outright" (as some countries have effectively done); nor is the U.S. saying that "every American, as a matter of right, is entitled to an unbreakable commercial encryption product." There is a false "tension" created in the assessment that this issue is an "either-or" proposition. Rather, both concerns can be, and in fact are, harmoniously balanced through a reasoned, balanced approach such as is proposed with the "Clipper Chip" and similar encryption techniques.

- Q: What does this decision indicate about how the Clinton Administration's policy toward encryption will differ from that of the Bush Administration?
- A: It indicates that we understand the importance of encryption technology in telecommunications and computing and are committed to working with industry and public-interest groups to find innovative ways to protect Americans' privacy, help businesses to compete, and ensure that law enforcement agencies have the tools they need to fight crime and terrorism.
- Q: Will the devices be exportable? Will other devices that use the government hardware?
- A: Voice encryption devices are subject to export control requirements. Case-by-case review for each export is required to ensure appropriate use of these devices. The same is true for other encryption devices. One of the attractions of this technology is the protection it can give to U.S. companies operating at home and abroad. With this in mind, we expect export licenses will be granted on a case-by-case basis for U.S. companies seeking to use these devices to secure their own communications abroad. We plan to review the possibility of permitting wider exportability of these products.

FACT SHEET

PUBLIC ENCRYPTION MANAGEMENT

The President has approved a directive on "Public Encryption Management." The directive provides for the following:

Advanced telecommunications and commercially available encryption are part of a wave of new computer and communications technology. Encryption products scramble information to protect the privacy of communications and data by preventing unauthorized access. Advanced telecommunications systems use digital technology to rapidly and precisely handle a high volume of communications. These advanced telecommunications systems are integral to the infrastructure needed to ensure economic competitiveness in the information age.

Despite its benefits, new communications technology can also frustrate lawful government electronic surveillance. Sophisticated encryption can have this effect in the United States. When exported abroad, it can be used to thwart foreign intelligence activities critical to our national interests. In the past, it has been possible to preserve a government capability to conduct electronic surveillance in furtherance of legitimate law enforcement and national security interests, while at the same time protecting the privacy and civil liberties of all citizens. As encryption technology improves, doing so will require new, innovative approaches.

In the area of communications encryption, the U.S. government has developed a microcircuit that not only provides privacy through encryption that is substantially more robust than the current government standard, but also permits escrowing of the keys needed to unlock the encryption. The system for the escrowing of keys will allow the government to gain access to encrypted information only with appropriate legal authorization.

To assist law enforcement and other government agencies to collect and decrypt, under legal authority, electronically transmitted information, I hereby direct the following action to be taken:

INSTALLATION OF GOVERNMENT-DEVELOPED MICROCIRCUITS

The Attorney General of the United States, or her representative, shall request manufacturers of communications hardware which incorporates encryption to install the U.S. government-developed key-escrow microcircuits in their products. The fact of law

enforcement access to the escrowed keys will not be concealed from the American public. All appropriate steps shall be taken to ensure that any existing or future versions of the key-escrow microcircuit are made widely available to U.S. communications hardware manufacturers, consistent with the need to ensure the security of the key-escrow system. In making this decision, I do not intend to prevent the private sector from developing, or the government from approving, other microcircuits or algorithms that are equally effective in assuring both privacy and a secure key-escrow system.

KEY-ESCROW

The Attorney General shall make all arrangements with appropriate entities to hold the keys for the key-escrow microcircuits installed in communications equipment. In each case, the key holder must agree to strict security procedures to prevent unauthorized release of the keys. The keys shall be released only to government agencies that have established their authority to acquire the content of those communications that have been encrypted by devices containing the microcircuits. The Attorney General shall review for legal sufficiency the procedures by which an agency establishes its authority to acquire the content of such communications.

PROCUREMENT AND USE OF ENCRYPTION DEVICES

The Secretary of Commerce, in consultation with other appropriate U.S. agencies, shall initiate a process to write standards to facilitate the procurement and use of encryption devices fitted with key-escrow microcircuits in federal communications systems that process sensitive but unclassified information. I expect this process to proceed on a schedule that will permit promulgation of a final standard within six months of this directive.

The Attorney General will procure and utilize encryption devices to the extent needed to preserve the government's ability to conduct lawful electronic surveillance and to fulfill the need for secure law enforcement communications. Further, the Attorney General shall utilize funds from the Department of Justice Asset Forfeiture Super Surplus Fund to effect this purchase.

More Details About the Clipper Chip

Q. How is the Clipper Chip used?

A. The chip performs a series of steps to encrypt or "scramble" the sender's data, which the recipient can unscramble by using a similar device also incorporating a Clipper Chip.

Several different "keys" are used within the chip and by the larger security devices. Normally these keys are transparent to the user. Law enforcement agencies, when properly authorized, can be given complementary pieces of one of these keys; to heighten security for the user, the pieces are held by two separate "key escrow agents." These two pieces then can be combined into one key with which the message can be unscrambled.

Q. What is contained in the Clipper Chip?

A. The chip is programmed with a classified encryption algorithm, a serial number, a chip unique key, and a chip family key.

Q. Specifically, how does the chip function?

A. The sender's data and encryption session key (generated each time communications between sender and receiver are initiated) is sent to the Clipper Chip. Next, the chip encrypts the data with the encryption key. It also encrypts the user's session key with the chip unique key and encrypts the serial number with the chip family key. All of this encrypted information becomes output from the chip to be sent to the receiver.

4/16/93

U.S. Technology Initiative for Secure Telephone Communications

Raymond G. Kammer
Acting Director
National Institute of Standards and Technology

April 16, 1993





Purpose

To Review the White House's Announcement of a new telephone encryption technology, the "**Clipper Chip**."

Summary of White House Announcement

- 1) New technology to improve telecommunications privacy and security;
- 2) Accelerate advanced telecommunications networks (NII);
- 3) Clipper Chip - new approach to encryption,
 - protects business secrets & privacy,
 - preserves law enforcement's ability to lawfully intercept communications of criminals;
- 4) Government purchase of products incorporating Clipper Chip technology; and
- 5) Government to work towards comprehensive encryption policy, consulting with Congress, industry, and interested individuals and organizations.



Why was the Clipper Chip developed?

1. To meet demands of business, individuals and government agencies for the cost-effective protection of information, such as:
 - trade secrets
 - sensitive phone calls
 - personal information
2. To protect American society by meeting legitimate needs of law enforcement for access to encrypted communications, as legally authorized. Specifically, to protect against:
 - terrorists
 - drug dealers
 - organized crime

What is the Clipper Chip?

The Clipper Chip is a computer encryption chip that will protect the privacy of American citizens and economic interests while accommodating law enforcement and national security needs. Specifically, Clipper Chip:

- provides stronger protection than the Data Encryption Standard, the current government standard;
- is designed to protect U.S. business communications against economic espionage;
- was developed by the government's foremost encryption technology experts;
- will be used by the U.S. Government to protect sensitive information, including defense and intelligence-related information;
- will protect the privacy of law-abiding Americans; and
- provides a mechanism for the secure escrowing of encryption keys, which can be used by law enforcement acting under appropriate legal authorization.



How does Clipper Chip balance the interests of privacy and law enforcement?

- The Clipper Chip meets the needs of both - a delicate balance.
- Excellent technical security

Advanced Government technique, development & testing process

Tougher to break:

Longer keys than DES (80 bits long vs. 56 for DES)

More possible keys

DES:

72,057,594,037,927,800

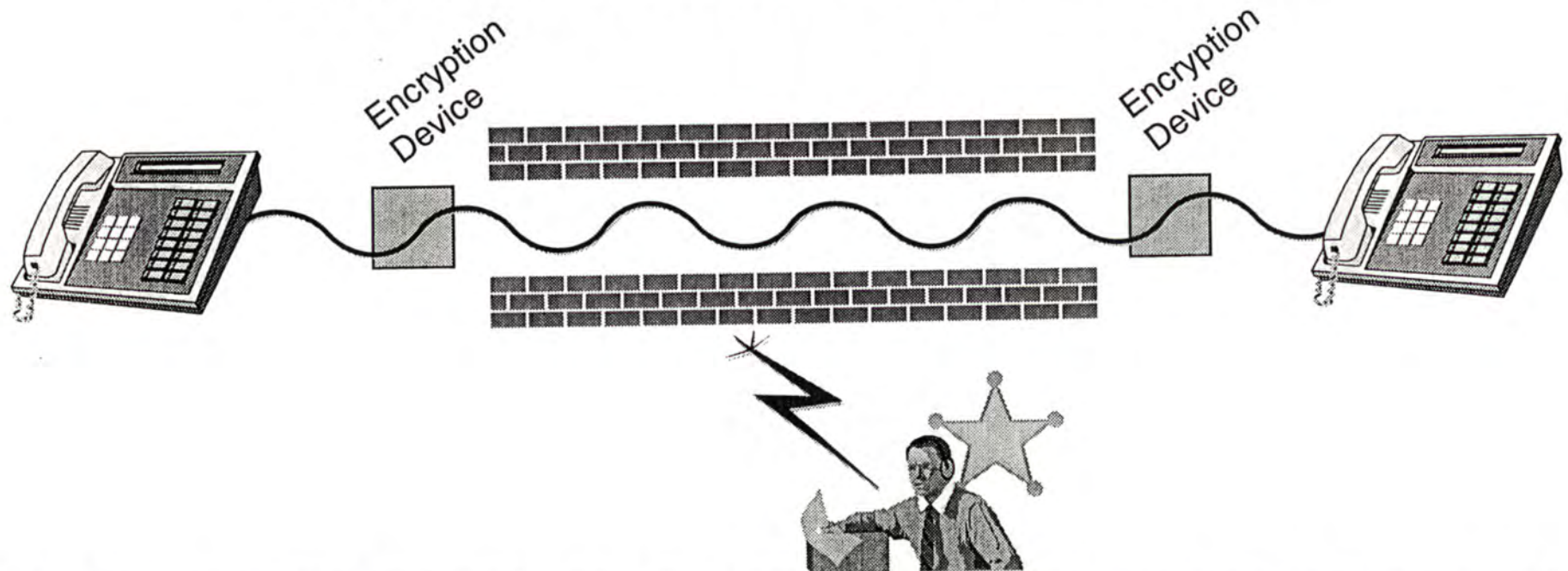
Clipper Chip: 1,208,925,747,557,040,000,000,000
(about 16 million times more than DES)

- mechanism for use only under legal authorization to obtain keys

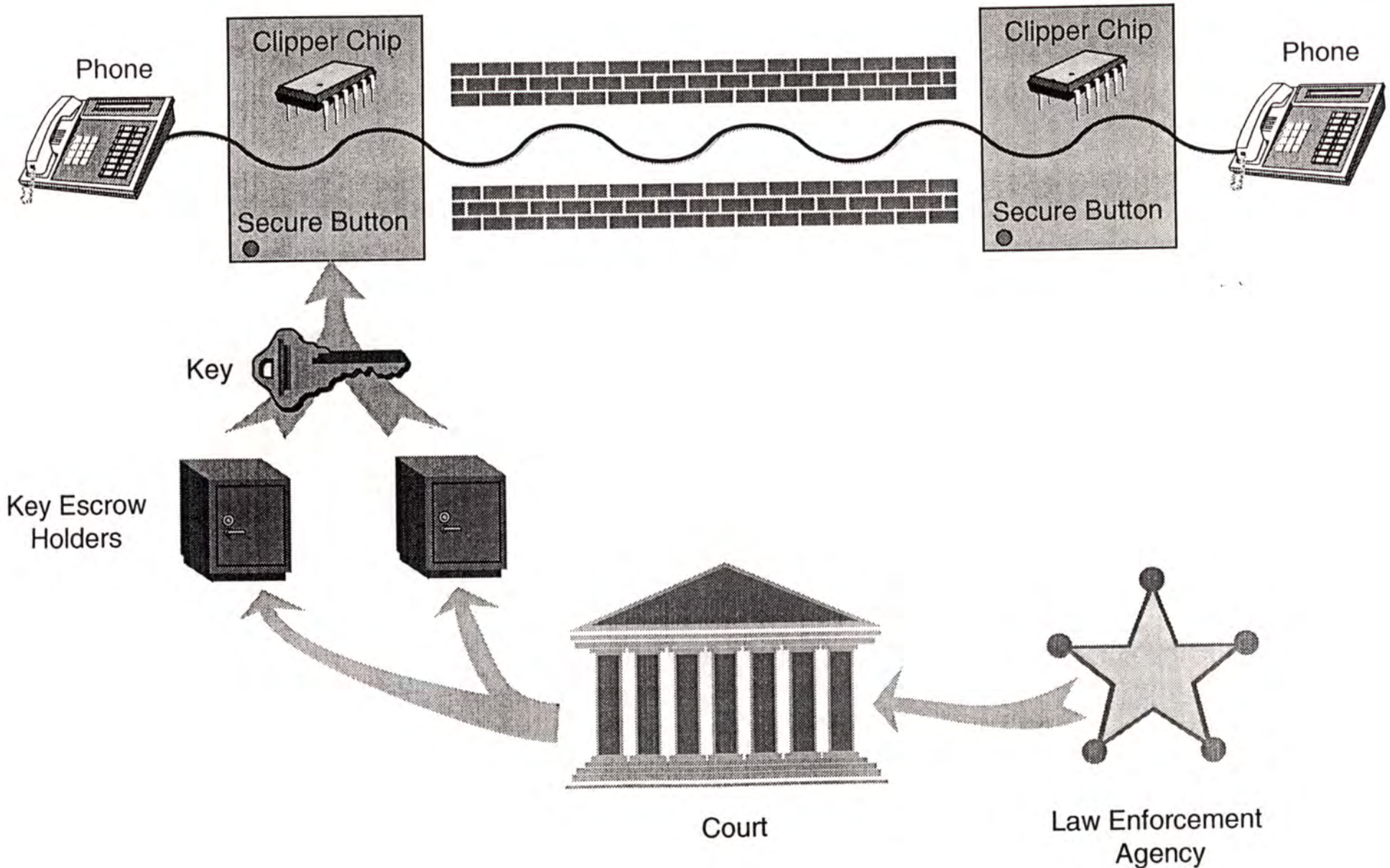
Industry's Problem



Law Enforcement's Problem



Clipper Chip Solution



What is NIST's Role?

- Under the Brooks Act and Computer Security Act of 1987, NIST develops cost-effective computer security standards to protect unclassified federal computer systems
- These standards also enjoy wide voluntary use in U.S. private sector
- Secretary of Commerce approves these standards as Federal Information Processing Standards
- President has directed Secretary of Commerce to develop standards that will implement this technology
- Adoption of this standard will allow federal agencies to facilitate rapid purchase and use of this technology by federal agencies

Conclusion

The new technology announced by the White House:

- strengthens individual privacy protection
- helps American industry
- addresses law enforcement's requirements, and
- achieves equitable balance

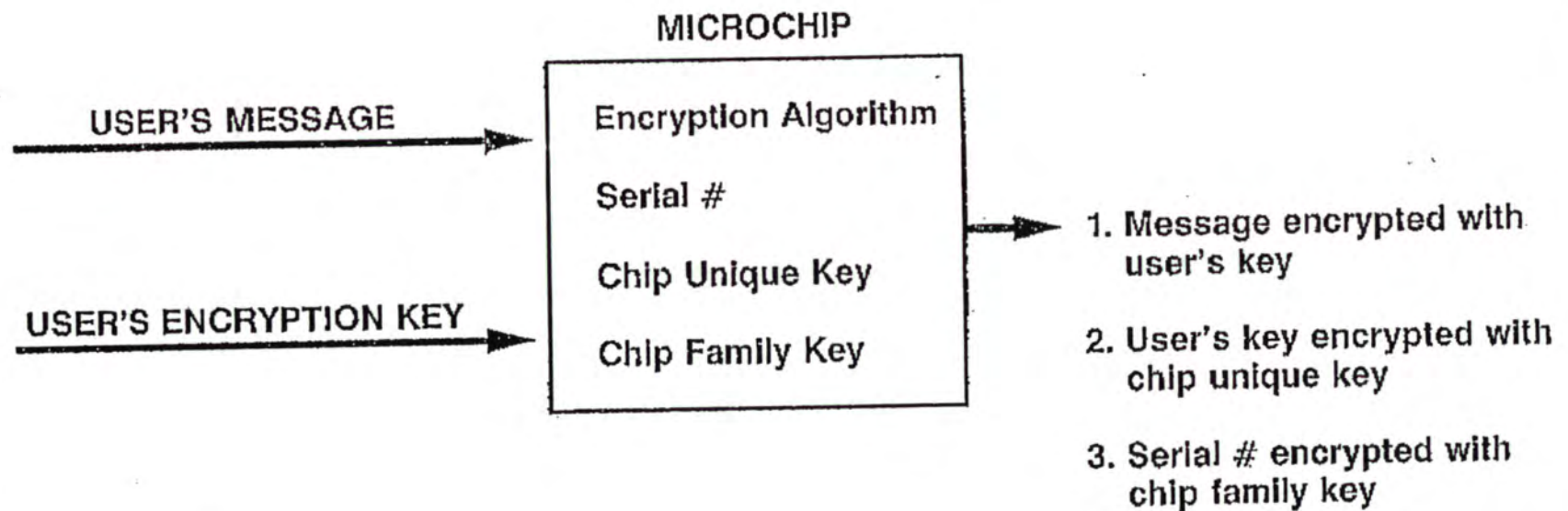
Review ordered by President will seek comprehensive policy on encryption to address:

- privacy of U.S. citizens, including need to use voice or data encryption for business purposes
- ability of government officials to access phone calls and data **under existing legal authority** when necessary to protect U.S. citizens
- effective and timely use of most advanced technology to build National Information Infrastructure and promote economic competitiveness and growth
- need for U.S. companies to manufacture and export high technology products

FOR LAW ENFORCEMENT TO READ A SUSPECT'S MESSAGE

1. Need to obtain court authorized warrant to tap the suspect's telephone
2. Record encrypted message
3. Use chip family key to decrypt chip serial number
4. Take this serial number and court order to custodians of disks A and B
5. Add the A and B components for that serial number = the chip unique key for the suspect user
6. Use this key to decrypt the user's message key for this recorded message
7. Finally, use this message key to decrypt the recorded message.

CHIP OPERATION



Cryptography, Clipper, and Capstone

Dorothy E. Denning¹
Georgetown University

Draft of May 11, 1993

1. Introduction

On April 16, 1993 the President announced a new technology initiative that will bring together the Federal Government and industry in a voluntary program to provide secure communications through strong cryptography while preserving law enforcement's ability to lawfully intercept communications through a key escrow arrangement. The plan is based on the development of a new tamper-proof encryption chip called the *Clipper Chip*² that implements an escrow-based encryption system.

The purpose of this article is to give an overview of the basic concepts of cryptography behind the new initiative, including single-key cryptography, public-key cryptography, key negotiation, authentication, and digital signatures; and to describe the new Clipper Chip and its successor *Capstone*, showing how the new chips can be used for secure communications, how law enforcement can obtain access to encrypted communications, and how the key escrow process might work.

Technical details and notation has been confined to footnotes and figures referenced through the footnotes. These can be skipped. For a more complete introduction to cryptography and the underlying mathematics, see for example [Denning 82].

2. Cryptosystems

Cryptography is the art and science of transforming (*encrypting*) information under secret keys for the purpose of secrecy or authenticity. A *cryptographic system* (*cryptosystem*) consists of encrypt and decrypt transformations (functions or algorithms) together with a set of keys that parameterize the transformations. The *encrypt* function scrambles data into what

¹Dorothy E. Denning is Professor and Chair of Computer Science at Georgetown University and author of *Cryptography and Data Security*. Her address is Georgetown University, Computer Science Department, 225 Reiss Building, Washington DC 20057; 202-687-5703; denning@cs.georgetown.edu. © 1993.

²The encryption chip has no relation to the microprocessor Clipper Chip of Intergraph Corporation.

appears as gibberish, while the *decrypt* function restores the original data. The original data is referred to as *plaintext* or *cleartext* and the scrambled data as *ciphertext*. The keys are not "hard-wired" into the functions, so the same functions can be used with different keys. At least the decrypt key must be kept secret to prevent an eavesdropper from decrypting intercepted ciphertext (the transformations themselves may be public). Figure 1 illustrates.

The *strength* of a cryptosystem refers to its ability to withstand attack by someone who intercepts the ciphertext. A system is *breakable* if it is possible to systematically determine the secret key needed to decrypt an intercepted ciphertext message. A system's strength depends on its underlying mathematics as well as the number of possible keys, which is determined by the key length (typically expressed as number of bits). For example, a 56-bit key has about 72,058 trillion possibilities. If the key length is too short, a system may be broken by brute force *exhaustive search*; that is, by systematically trying all possible keys until one is found that produces meaningful plaintext or, even better, some known plaintext. The process of attempting to break a cryptosystem is called *cryptanalysis*.

With one exception, all cryptosystems are at least theoretically breakable given sufficient resources. The exception is the *one-time pad*, which uses a key as long as the message and never uses the same key more than once. In digital systems, the key and message are both streams of bits (each text character is 8 bits) and each key bit is XORed (exclusive-or'ed) with the corresponding message bit to produce a ciphertext bit. The XOR operation yields 0 if both bits are the same (i.e., 00 or 11) and 1 if they are different (01 or 10) as illustrated by the following:

message stream	01101101 ...
key stream	10110001 ...
ciphertext stream	11011100 ...

Decryption is identical except that the key bits are XORed with the ciphertext bits. The reason it is unbreakable is because for any given ciphertext stream, there is some key stream that will produce any possible message stream of that length. The one-time pad and systems that simulate it are called *stream ciphers* because they operate on streams of bits (or 8-bit characters).

While theoretically breakable, many systems are *computationally strong* or *practically unbreakable* in the sense that the resources required to do so are unavailable or prohibitively expensive. In practice, a system need only be strong enough to provide security commensurate with the risk and consequences of breakage. Increasing security usually increases costs and decreases performance, so it does not make sense to pay more for encryption than the expected loss resulting from breakage.

There are two types of cryptosystems: single-key and public-key.

3. Single-Key Cryptosystems

A *single-key cryptosystem* is one where the encryption and decryption keys are the same (or readily derived from each other) and kept secret. Single-key systems are also called *secret-key* systems and *symmetric* systems. Since all publicly known cryptosystems prior to the late 70's were single-key systems, they are also called *traditional* or *conventional cryptosystems*. Figure 2 illustrates.

In addition to secrecy, requirements for secure communications often include *authenticity*: protection against message tampering or injection of bogus messages by a third party. Single-key cryptosystems provide authenticity because the secret key is needed to modify or create ciphertext that decrypts into meaningful plaintext. If meaningful plaintext is not automatically recognizable, then a *message authentication code* (MAC) can be computed and appended to the message. The computation is a function of the entire message and a secret key, and has the property that it is practically impossible to find another message with the same authenticator. The receiver checks the authenticity of the message by computing the MAC using the same secret key and then verifying that the computed value is the same as the one transmitted with the message. A MAC can be used to provide authenticity for unencrypted messages as well as for encrypted ones. NIST has adopted a standard for computing a MAC [NIST FIPS 113].

Single-key systems are often used during the process of *authenticating users* to a system. Systems that use passwords usually store those passwords in encrypted form using the password as the key so that the ciphertext passwords cannot be decrypted. When encryption is used this way, it effectively implements a one-way function of the secret information that cannot be reversed. (If a password is forgotten, it is replaced with a new one.) Stronger forms of user authentication are possible using access tokens and smart cards that have cryptographic capabilities.

Single-key cryptosystems have been used extensively by the government, particularly the defense and intelligence communities, to protect classified communications. The methods used for this purpose are also classified. For example, the STU-III, which is used for classified telephone conversations, implements a classified single-key encryption system.

3.1 The Data Encryption Standard

The Data Encryption Standard (DES), developed by IBM and adopted by the National Institute of Standards and Technology (NIST) as a government standard in 1977 [NIST FIPS 46-1], is a single-key system that encrypts 64-bit blocks with a 56-bit key. After an initial permutation of the bits, a plaintext block goes through 16 iterations ("rounds") of a complex function and then passes through a final permutation that yields the ciphertext block. During each round, the bits undergo further permutations and are transformed by "S-boxes" which define bit substitutions. The security of the algorithm depends on the S-boxes, the number of iterations, and the key length. The algorithm is public knowledge, though the design of the

S-boxes is classified. Hardware implementations of DES run in excess of one gigabit per second.

DES can be used in four different operating modes:

1. *Electronic Codebook* (ECB), which encrypts 64-bit blocks as independent units.
2. *Output Feedback* (OFB), which uses DES to generate a key stream that is XORed with the message stream to simulate a one-time pad. The key stream is generated by encrypting an initialization block with DES under a secret key to produce a segment of key bits, and then repeatedly feeding those DES output bits back into DES as input to generate another segment of key bits.
3. *Cipher Feedback* (CFB), which is also a stream cipher except that the ciphertext is fed back into the DES key generator so that each encryption depends on previous ciphertext.
4. *Cipher Block Chaining* (CBC), which encrypts 64-bit blocks but chains them together by XORing each ciphertext block with the next plaintext block before encrypting the plaintext block.

When DES was first introduced in 1975, some critics argued that 56-bit keys were too short and that the S-boxes, which are a critical part of the algorithm, were suspect because of involvement by the NSA and because the design documents had been classified. Diffie and Hellman [Diffie & Hellman 77] claimed that DES could in principle be broken by exhaustive search with a \$20 million machine containing a million processors, and that this was unacceptable for a national standard. Hellman went so far as to claim that DES would be totally insecure within ten years [Hellman 79]. Eighteen years later, DES has withstood considerable public scrutiny and many efforts to attack it. Moreover, analysis has shown that the key size is appropriate for the number of rounds and that the S-boxes are well-designed and without trapdoors [Denning 90]. Claims that DES is weak remain unsubstantiated, and DES is likely to be recertified as a government standard for another five years.

Additional security can be achieved by using two keys in double or triple encryption mode. In *triple encryption mode*, the message block is first encrypted under the first key, then decrypted under the second key, and finally encrypted again under the first key (the decrypt step does not undo the encrypt step since different keys are used).

DES was adopted as a government standard to protect sensitive but unclassified information. It has also been adopted as a standard outside the government. The American National Standards Institute (ANSI) has adopted standards for encryption, access control, and key management that use DES. PEM (Privacy Enhanced Mail), the Internet standard for protecting electronic mail, uses DES to encrypt electronic mail messages on the Internet.

Products with DES generally are not exportable except on an individual sale basis and in certain applications, for example banking and authentication, where the DES is not used for message secrecy. RSA Data Security, Inc. has developed two single-key cryptosystems, RC2 and RC4, which use 40-bit keys and can be exported through a general licensing agreement. RC2 operates as a block cipher, that is, in ECB mode, while RC4 operates as a stream cipher. These systems have been incorporated into some software packages, for example, RC2 in Lotus Notes to encrypt documents, and RC4 in Novelle's Netware version 4.0.

3.2 The Clipper Chip

The Clipper Chip contains a 64-bit block encryption algorithm called *Skipjack*, designed by NSA and classified SECRET. The Skipjack algorithm uses 80-bit keys and has 32 rounds of scrambling. Thus, Skipjack is stronger than DES, having about sixteen million times more keys and twice as much scrambling. It supports all four DES modes of operation. Mykotronx's "MYK-78" implementation runs at 12 megabits per second in Electronic Codebook (ECB) mode.

Each chip includes the following components, the last four of which are written into a special memory (called VROM or VIA-LINK) on the chip when it is programmed:

1. the Skipjack encryption algorithm
2. an 80-bit *family key* that is common to all chips and used by law enforcement
3. a 25 to 30-bit *serial number* (the exact length has not yet been determined)
4. an 80-bit secret *unit key* that unlocks all messages encrypted with the chip
5. specialized control software

Each 80-bit unit key is stored in escrow with two or more trusted agencies as a "split key." Here we will assume that two trustees are used, although this is subject to change. Each "half" of a split key is a full 80 bits, and the two halves are XORed together to recover the unit key as shown in Figure 3. Knowing one half is insufficient to determine the unit key since the second half could be any 80 bits.

The key escrow process is coupled to the process of key generation and chip programming, which takes place inside a vault. Although the exact process has not yet been determined, the following outlines a possible approach. At the beginning of a session, a trusted agent from each of the two key escrow agencies enters the vault. The first enters a secret, random 80-bit value into a laptop computer and the second agent enters a second secret, random value. These random values serve as seeds to generate unit keys and their key halves for a sequence of serial numbers.³ Thus, the unit keys are a function of 160 secret, random bits, where each

³To generate the unit key U for a serial number N , the value of N is first padded with a fixed block to produce a 64-bit block NI . The seeds $S1$ and $S2$ entered by the agents are then used as keys to triple-encrypt NI , producing a 64-bit block RI :

agent knows only 80. As a sequence of unit keys and key halves are generated, they are written onto three separate floppy disks along with their serial numbers. The escrow agents each get one of the disks with the key halves. The disk with the unit keys is used by the programming equipment to put the serial numbers and unit keys onto the chips.⁴

After the chips are programmed, all information is discarded from the vault and the agents leave. The protocol may be changed slightly so that four people are in the room instead of two. The first two would provide the seeds and the second two (the escrow agents) would take the disks back to the escrow agencies.

The Clipper Chip is intended to become a government standard for sensitive but unclassified information. The first product to incorporate the new chip is the AT&T Telephone Security Device, which provides secure voice and data communications.

3.3 Negotiating a Session Key

In order to use the Clipper Chip (or any other single-key cryptosystem) to encrypt communications, the two parties must first agree on a secret *session key*, that is, a key for encrypting all communications transmitted in either direction. The process of establishing a session key is called *key negotiation*, *distribution*, or *exchange*.

A *public-key distribution system* allows the security devices operating on behalf of two parties to negotiate a secret session key without exchanging any secret values. Figure 6 illustrates.

$$R1 = E_{S1}(D_{S2}(E_{S1}(N1))) .$$

Similarly, N is padded with two other fixed blocks to produce $N2$ and $N3$, and two additional 64-bit blocks $R2$ and $R3$ are computed:

$$\begin{aligned} R2 &= E_{S1}(D_{S2}(E_{S1}(N2))) \\ R3 &= E_{S1}(D_{S2}(E_{S1}(N3))) . \end{aligned}$$

$R1$, $R2$, and $R3$ are then concatenated together, giving 192 bits. The first 80 bits are assigned to the first key half $U1$ and the second 80 bits to the second key half $U2$. The rest are discarded. The unit key U is the XOR of $U1$ and $U2$. Figure 4 illustrates.

⁴Figure 5 illustrates the entire process of key generation, key escrow, and chip programming. The first floppy disk, which is taken by the first escrow agent, contains a file for each serial number N that contains the corresponding key part $U1$. The second disk, which is taken by the second agent, is similar but contains the $U2$ values. The third disk, which is used to program the chips, contains the unit keys U . The programmed chips also contain the encryption algorithm E , family key F , and control software (not shown).

Each device generates a "private key" that is a random, secret value. Next it computes a one-way function of that value which results in a "public key." The one-way function has the property that it is practically impossible to reverse the function; that is, to compute the private key from the public key. The two devices then exchange their public keys. Finally, each device computes a function of its private key and the public key received from the other device. The result is a common session key that is a function of both private keys. An eavesdropper observing the exchange will be unable to determine the private keys and, thus, the session key.⁵

The AT&T telephone security device, which includes the Clipper Chip, uses a proprietary public-key distribution method to set up a session key for a secure conversation. The key negotiation takes place without the Clipper Chip.

A public-key cryptosystem (Section 4) can also be used to establish a session key. In this case, the key is picked by one user and transmitted to the other using the public-key system.

3.4 Encrypting with the Clipper Chip

Once an 80-bit session key is established for use with the Clipper Chip, it is sent to the chip. The chip then encrypts the session key with the unit key and concatenates the 80-bit result with the serial number and authentication pattern for a total of 128 bits (for a 25-bit serial number, the authentication pattern is 23 bits). The 128-bit block is then encrypted under the chip's family key to produce a 128-bit cipher block chain called the *Law Enforcement Field*

⁵Figure 7 illustrates a public-key distribution method invented by Diffie and Hellman [Diffie & Hellman 76]. User *A* generates a random, private key x_A and user *B* generates a random, private key x_B . Then *A* computes a public key y_A from x_A , and *B* computes a public key y_B from x_B as follows:

$$A: y_A = g^{x_A} \bmod p$$

$$B: y_B = g^{x_B} \bmod p$$

where p is a global prime and g is a second global number. Arithmetic is done modulo p (i.e., all numbers are in the range from 0 through $p - 1$ and when a computation yields a result in excess of $p - 1$, the result is divided by p and replaced by the remainder). The users then exchange their public y values and use them to generate a common key K that is a function of both x values:

$$A: K = y_B^{x_A} \bmod p = g^{x_A x_B} \bmod p$$

$$B: K = y_A^{x_B} \bmod p = g^{x_A x_B} \bmod p$$

An eavesdropper intercepting the y values will be unable to compute the key K since he or she will lack the appropriate x value. Although in theory x can be computed from its related y value by taking the discrete log (i.e., the $\log \bmod p$), in practice this is intractable for large p , say 700 bits or more.

(LEF).⁶ The LEF is transmitted to the receiving chip at least once and used together with a random initialization block to establish synchronization. Once synchronized, the session key is used to encrypt and decrypt messages in both directions. For voice communications, the message stream (voice) is first digitized. Figure 8 shows the transmission of the LEF and encrypted message stream from a sender *A*'s security device containing a Clipper Chip to a receiver *B*'s device.

3.5 Law Enforcement Access

When a law enforcement officer has been granted a court order authorizing a tap on a particular line, the officer will first take the warrant to the service provider in order to get access to the communications associated with that line. Let us assume that the tap is in place and that communications encrypted with the Clipper Chip have been intercepted as shown in Figure 8. A special decoder box will extract the Law Enforcement Field, decrypt it with the family key, and extract the serial number of the chip. The law enforcement officer will then send (e.g., via secure FAX) each of the key escrow agencies a request for the key half it is holding for the given serial number together with documentation certifying that a tap has been authorized for the party associated with that serial number. When the two halves of the chip's unit key are returned, they will be XORed together to produce the unit key.⁷ The unit key will then be used to decrypt the session key in the LEF. Finally, the decoder will decrypt the communications.

4. Public-Key Cryptosystems

A *public-key cryptosystem* (or *asymmetric system*) is one where each user (or application) has a pair of permanent (or long-term) keys: a *public key* and a *private key*. The public key can be freely distributed or stored in a public directory, while the private key must be known only to the user (or the user's cryptographic chip). Because the public and private keys must be mathematically related, it must also be the case that the private key cannot be derived from the public key. The concept of public-key cryptography was proposed by Diffie and Hellman in 1976 [Diffie & Hellman 76].

⁶The LEF contains $E_{UA}(K)$, namely the session key K encrypted under the unit key UA of *A*'s device, concatenated with the serial number NA and authentication pattern PA , all encrypted under the common family key F :

$$E_F(E_{UA}(K), NA, PA) \quad .$$

⁷For serial number NA , the first escrow agency returns the key half UIA and the second returns $U2A$. The unit key U is the XOR of UIA and $U2A$.

The advantage of public-key systems is that they allow the transmission of secret messages without the need to exchange a secret key. To send a message, the sender obtains the receiver's public key and uses it to encrypt the message. The receiver then decrypts the message using its private key. The sender's keys are not used (they would be used in a reply). Figure 9 illustrates.

Public-key cryptosystems can provide secrecy but not authenticity. This is because a third party, with access to the receiver's public encryption key, could inject bogus ciphertext that would decrypt into meaningful plaintext. To get authenticity, it is necessary to combine a public-key cryptosystem with a public-key signature system (Section 5).

4.1 The RSA System

Rivest, Shamir, and Adleman invented the first (publicly known) public-key system (now called "RSA") [Rivest, Shamir & Adleman 78]. Encryption and decryption are both performed by raising a large message block to an exponent in modular arithmetic. A public key consists of a modulus, which is the product of two large secret primes, and an exponent. The corresponding private key consists of the modulus, the primes, and a secret exponent that cannot be determined without knowing the primes. The key size is on the order of 512 to 1024 bits. The exponents are related in such a way that applying them in succession restores the original message. An adversary, knowing the public key, cannot determine the primes without factoring the modulus, which is thought to be intractable for large numbers.⁸

The RSA cryptosystem is considerably more time consuming than single-key systems, which typically use simple permutations and substitutions of bits. For this reason, it is not recommended for encrypting general communications or data. However, it is recommended for distributing the session keys used with single-key systems. To send an encrypted message, the sender generates a session key, encrypts the message under the session key using the single-key system, and encrypts the session key under the receiver's public key using RSA. The RSA-encrypted session key is then transmitted along with the encrypted message. Internet Privacy Enhanced Mail (PEM) uses RSA and DES in this way to encrypt electronic mail messages. It also uses RSA to compute digital signatures for messages.

4.2 Fair Public-Key Cryptosystems

A *fair public-key cryptosystem* is one with an objective similar to the Clipper Chip, namely to provide strong encryption for privacy and security while at the same time allowing law enforcement access when legally authorized. The concept, introduced by Silvio Micali [Micali 92], is realized by splitting each private key into multiple parts, and registering each

⁸Figure 10 illustrates. The public key consists of a modulus n , where $n = pq$ for secret primes p and q , and exponent e ; and the private key consists of n , p , q , and a secret exponent d that is the inverse of $e \bmod (p-1)(q-1)$. A message block M is encrypted by raising it to the exponent $e \bmod n$ and then decrypted by raising it to the exponent $d \bmod n$.

part with a separate key escrow agency as with Clipper. It differs from Clipper in that the key parts are generated and distributed in such a way that a key management center can verify in advance that the distributed parts, when combined, will produce the original key. This is done using only the public key and other public information derived from the key parts. This method of key escrow cannot be used with a single-key system such as the Clipper Chip.

5. Digital Signature Systems

A *digital signature* is a block of data attached to a message (document, file, record, etc.) that binds the message to a particular individual (or entity) such that the signature can be verified by the receiver or independent third party (e.g., judge) and such that it cannot be forged. The binding is accomplished through a *digital signature system* which is like a public-key cryptosystem in that each user has a public-private key pair that is used with a pair of functions. A message is "signed" by applying a "signature" function, keyed to the signer's private key, to the message. The result is the digital signature for the message. The signature is verified by applying the "verification" function, keyed to the signer's public key, to the message and signature. The message itself may be passed in the clear or encrypted using some other method. Figure 11 illustrates.

Digital signatures provide *non-repudiation* in that the signer cannot falsely deny having originated the message. Thus, they can be used to sign electronic contracts, purchase orders, and other legally binding documents in the same way that written signatures are used to sign such documents. In addition, digital signatures can be used to authenticate software (e.g., to protect against computer viruses), data, images, users, and machines.

Rather than applying the signature function to an entire message, it is customary to first compute a condensed *digest* of the message using a public *hash function* and then sign the digest. This speeds up the signing process and allows the signature to be shorter than the message. The receiver likewise hashes the message before verifying the signature. This is shown in Figure 12. The hash function must have the property that it is practically impossible to find a second message with the same digest or to find two different messages that produce the same digest. The first condition prevents someone else from claiming that a different message was signed while the second condition prevents the signer from making such a claim later. The Secure Hash Algorithm (SHA), which condenses a message to 160 bits, has been adopted as the government standard [NIST FIPS 180].

The RSA public-key system can be used as a signature system as well as a cryptosystem. This is because the encryption and decryption algorithms are identical.⁹

⁹Figure 13 shows how RSA is used as a signature system.

5.1 The Digital Signature Standard

In 1991, NIST proposed a Digital Signature Standard (DSS) for government systems [NIST 91]. Unlike RSA, the DSS is strictly a signature system; it cannot be used as a cryptosystem for message secrecy. It uses the Secure Hash Algorithm (SHA) to condense a message before signing.¹⁰

The DSS performs exponentiations of large numbers in modular arithmetic. The key size is 512-1024 bits, and security depends on the difficulty of inverting the exponentiations; that is computing logs in modular arithmetic. This is approximately the same as factoring, so the security of DSS is comparable to that of RSA.

5.2 Public-Key Certificates

Public-key cryptosystems and signature systems are attractive because of their ability to achieve secrecy by exchanging only public information. There is, however, a security risk with public keys, namely the substitution of fake public keys. For example, suppose that a masquerader substitutes his or her own public key for that of some other person. Then, unwittingly, others may accept signatures created by the masquerader, believing them to be from the masquerader's victim.

To protect against this threat, public keys can be packaged in *certificates* that serve to validate the keys. A certificate typically contains the user's identification, public key, and a time/date stamp. It is digitally signed by a *certification authority*, whose public key must be protected

¹⁰Figure 14 illustrates. Each user has a private key x that is 512-1024 bits and a public key consisting of four values: y , p , q , and g where $y = g^x \bmod p$ (thus x is the discrete log of y base g in $\bmod p$). All values are of the key size except for q and x , which are 160 bits. The public values p , q , and g may be shared within a group. To sign a message m , a user picks a random value k (the message key) and uses it along with x , p , q , and g to compute:

$$\begin{aligned}r &= (g^k \bmod p) \bmod q \\s &= (k^{-1}(H(m) + xr)) \bmod q\end{aligned}$$

where H is the Secure Hash Algorithm (SHA), which computes a 160-bit digest of m . Both r and s constitute the signature. The signature is validated by computing:

$$\begin{aligned}w &= s^{-1} \bmod q \\u1 &= H(m)w \bmod q \\u2 &= rw \bmod q \\v &= (g^{u1}y^{u2} \bmod p) \bmod q.\end{aligned}$$

If the value v produced in the last step is the same as r , then the signature is accepted as valid; otherwise it is rejected as a forgery. See [NIST 91] for a complete description of the mathematics and a proof that $v = r$ when the signature is legitimate.

by some other means. Before using a public key, the certificate is validated (i.e., its signature is checked). In the case of a digital signature, the user may send the certificate along with the signature to the certification authority for verification. NIST has initiated a study to develop a National Digital Signature Certification Authority for validating keys and signatures.

6. The Capstone Chip

The Capstone Chip combines the capabilities of the Clipper Chip for encryption, key escrow, and law enforcement access with the following functions for negotiating session keys and signing messages:

1. The Digital Signature Algorithm (DSA) used with the DSS.
2. The Secure Hashing Algorithm (SHA), also used with the DSS.
3. A key negotiation algorithm based on a public key exchange.
4. A general purpose exponentiation algorithm.
5. A random number generator that uses a pure noise source.

The Capstone Chip will initially be used by the Preliminary Message Security Protocol in the Defense Messaging System.

References

Denning, D.E., *Cryptography and Data Security*, Addison-Wesley, 1982.

Denning, D. E., *The Data Encryption Standard: Fifteen Years of Public Scrutiny*, Proc. Sixth Annual Computer Security Applications Conf., IEEE Computer Society Press, Dec. 3-7, 1990.

Diffie, W. and Hellman, M., "New Directions in Cryptography," *IEEE Trans. on Info. Theory* Vol IT-22(6), Nov. 1976, pp. 644-654.

Diffie, W. and Hellman, M., "Exhaustive Cryptanalysis of the NBS Data Encryption Standard," *Computer*, Vol. 10(6), June 1977, pp. 74-84.

Hellman, M. E., "DES Will Be Totally Insecure Within Ten Years," *IEEE Spectrum*, Vol 16 (7), July 1979, pp. 32-39.

Micali, S., "Fair Public-Key Cryptosystems," Laboratory for Computer Science, MIT, Aug.

21, 199.

National Institute for Standards and Technology, "Computer Data Authentication," Federal Information Processing Standards Publication (FIPS PUB) 113.

National Institute for Standards and Technology, "Data Encryption Standard (DES)," Federal Information Processing Standards Publication (FIPS PUB) 46-1, April 1977, National Technical Information Services, Springfield, VA.

National Institute for Standards and Technology, "DES Modes of Operation," Federal Information Processing Standards Publication (FIPS PUB) 81, Dec. 1980, National Technical Information Services, Springfield, VA.

National Institute for Standards and Technology, "A Proposed Federal Information Processing Standard for Digital Signature Standard (DSS)," *Federal Register*, Vol. 56, Aug. 1991, p. 169.

National Institute for Standards and Technology, "Specifications for the Secure Hash Standard," Federal Information Processing Standards Publication (FIPS PUB) 180 (draft), Oct. 30, 1992.

Rivest, R. L., Shamir, A., and Adleman, L., "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," *Comm. ACM*, Vol 21(2), Feb. 1978, pp. 120-128.

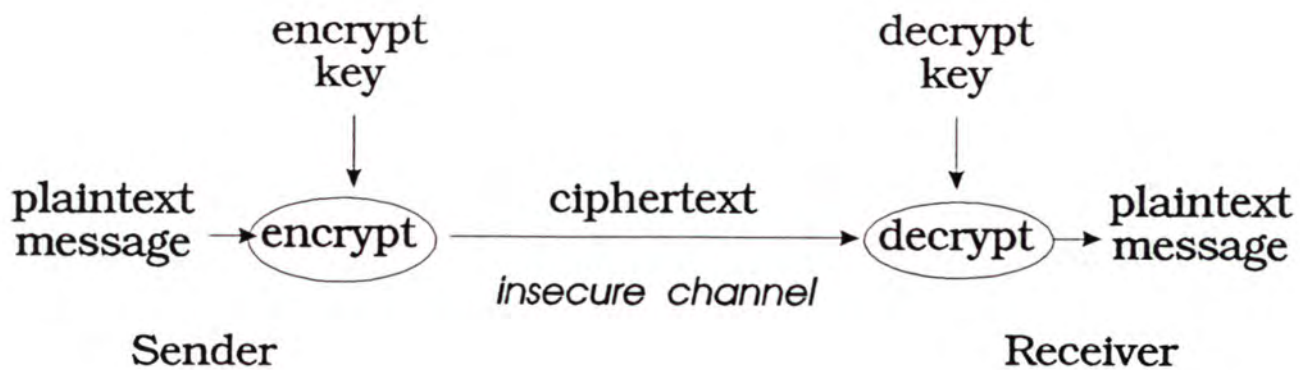


Figure 1. Cryptosystem.

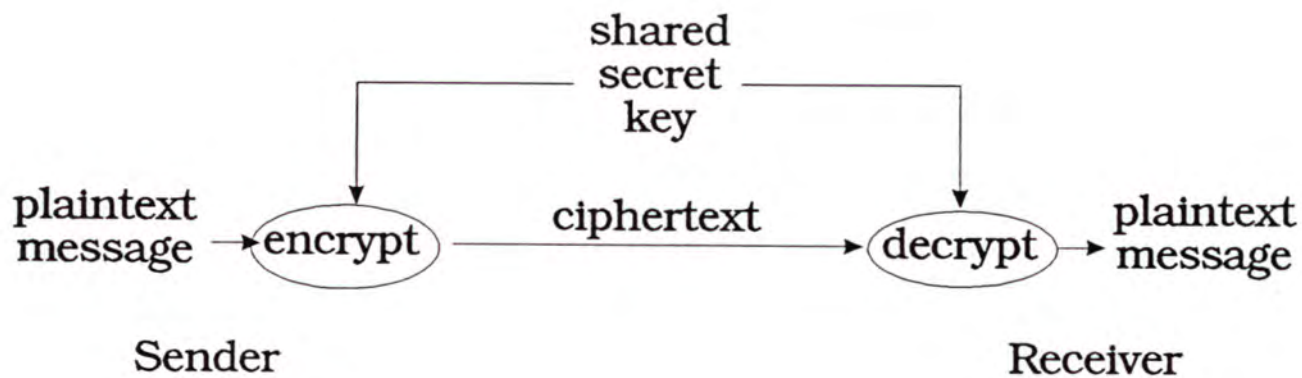


Figure 2. Single-Key Cryptosystem.

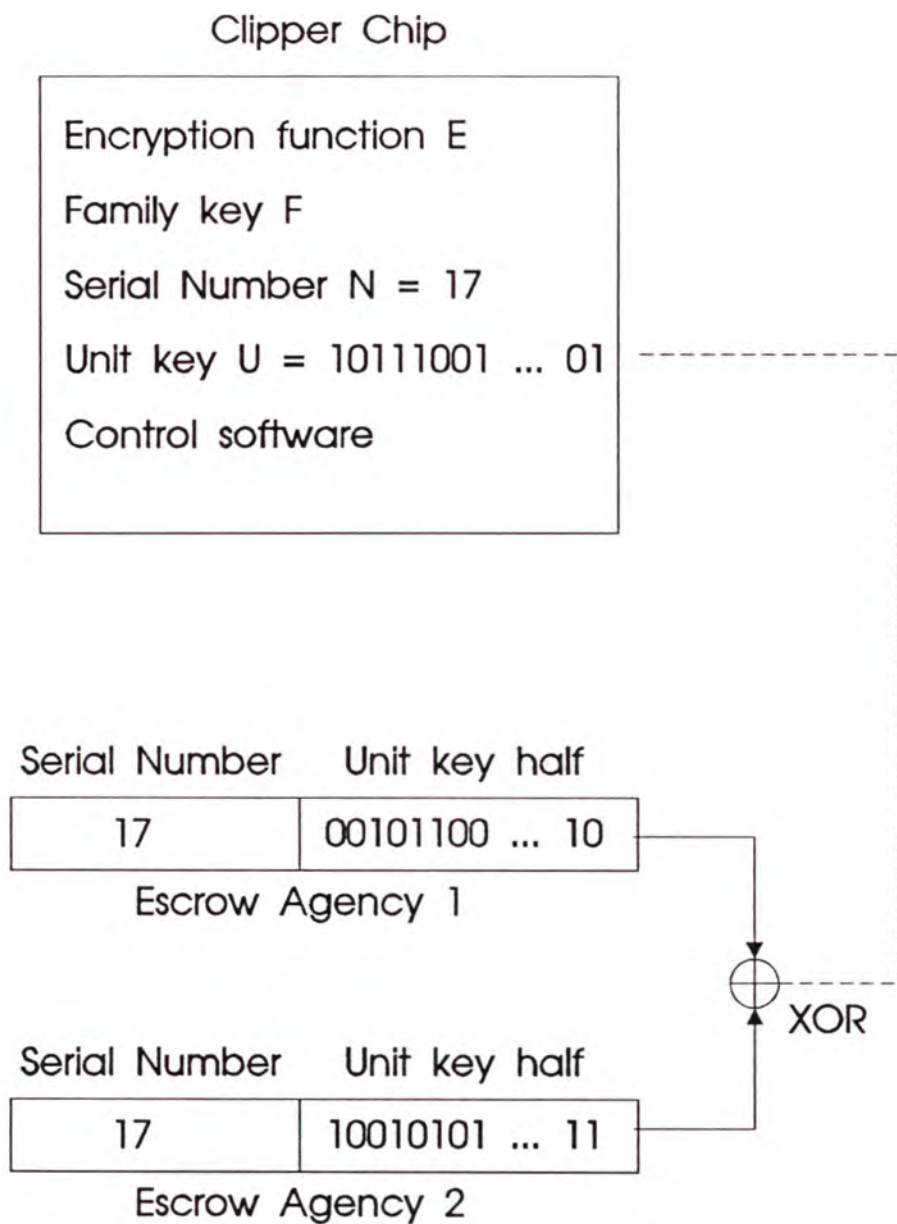


Figure 3. Clipper Chip with Split-Key Escrow.

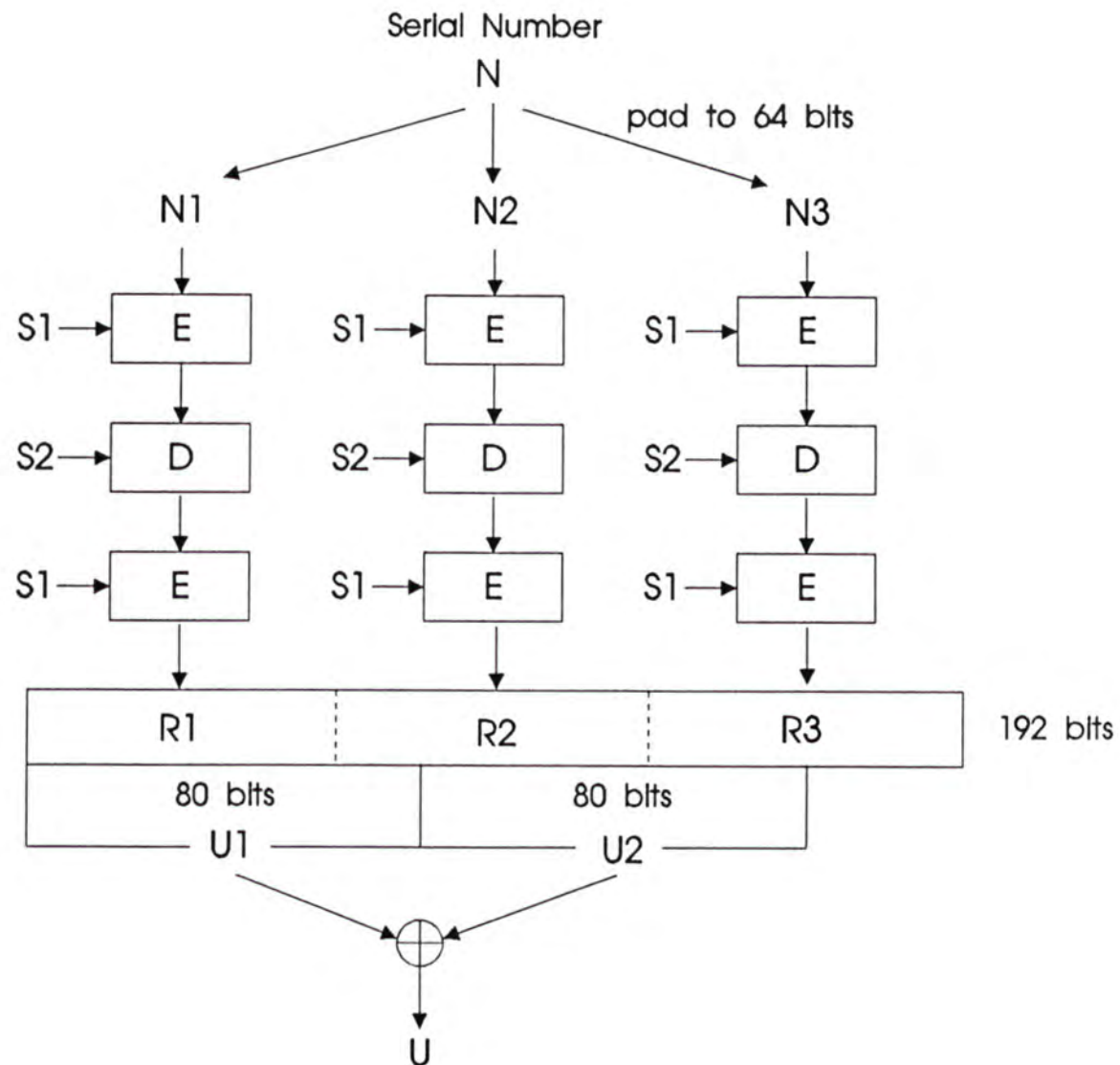


Figure 4. Generation of Unit Key U and Key Parts $U1$, $U2$.

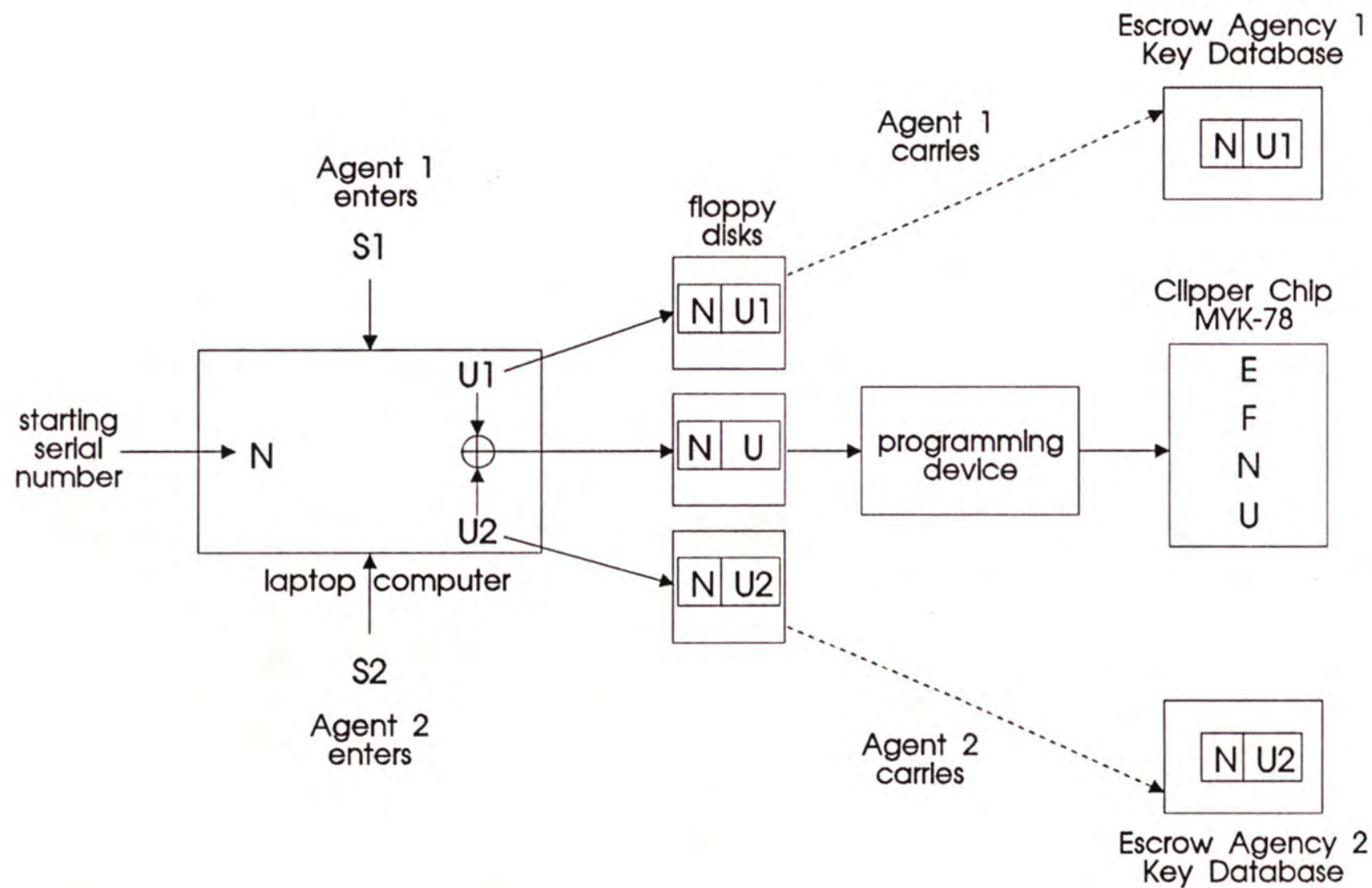


Figure 5. Chip Programming and Key Escrow.

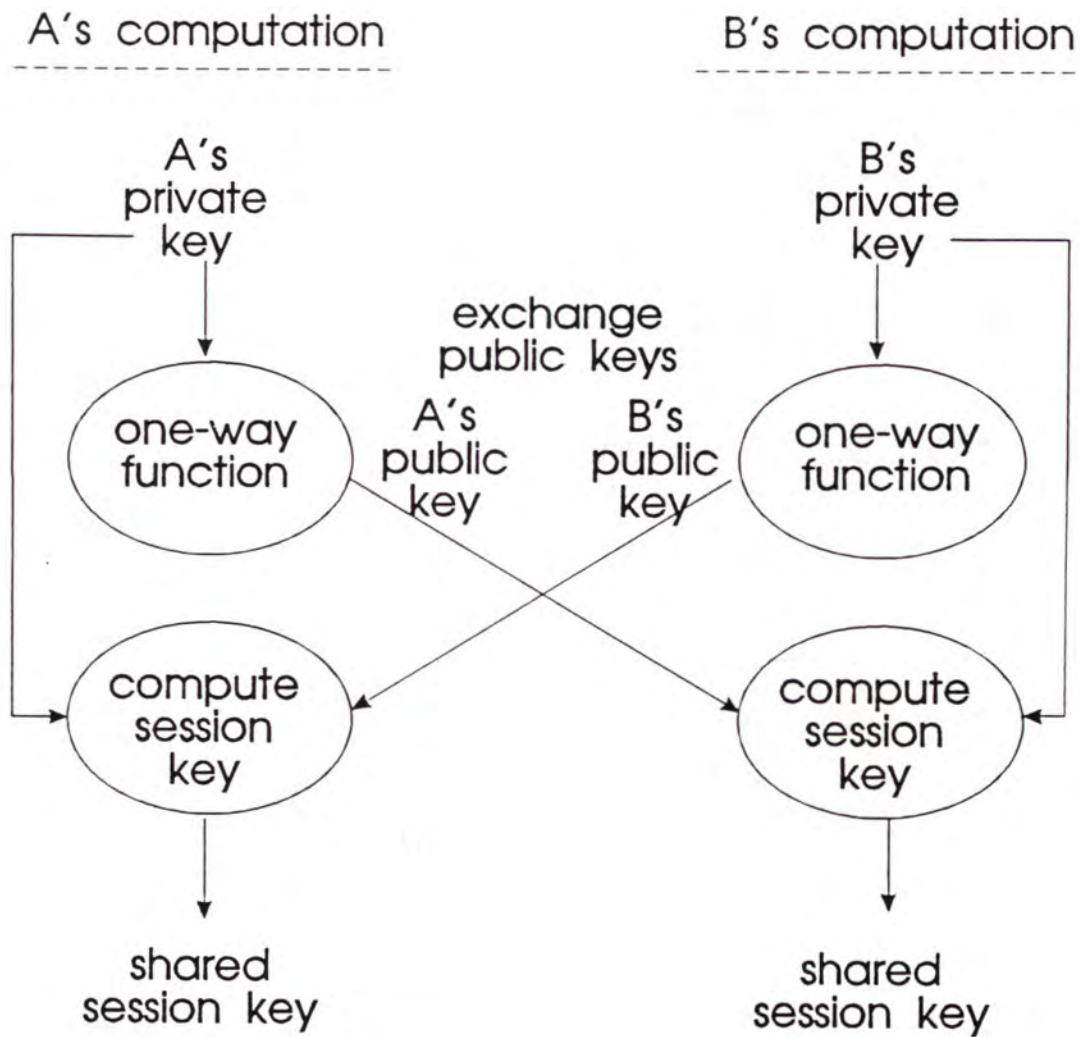


Figure 6.

Key Negotiation Using a Public-Key Distribution System.

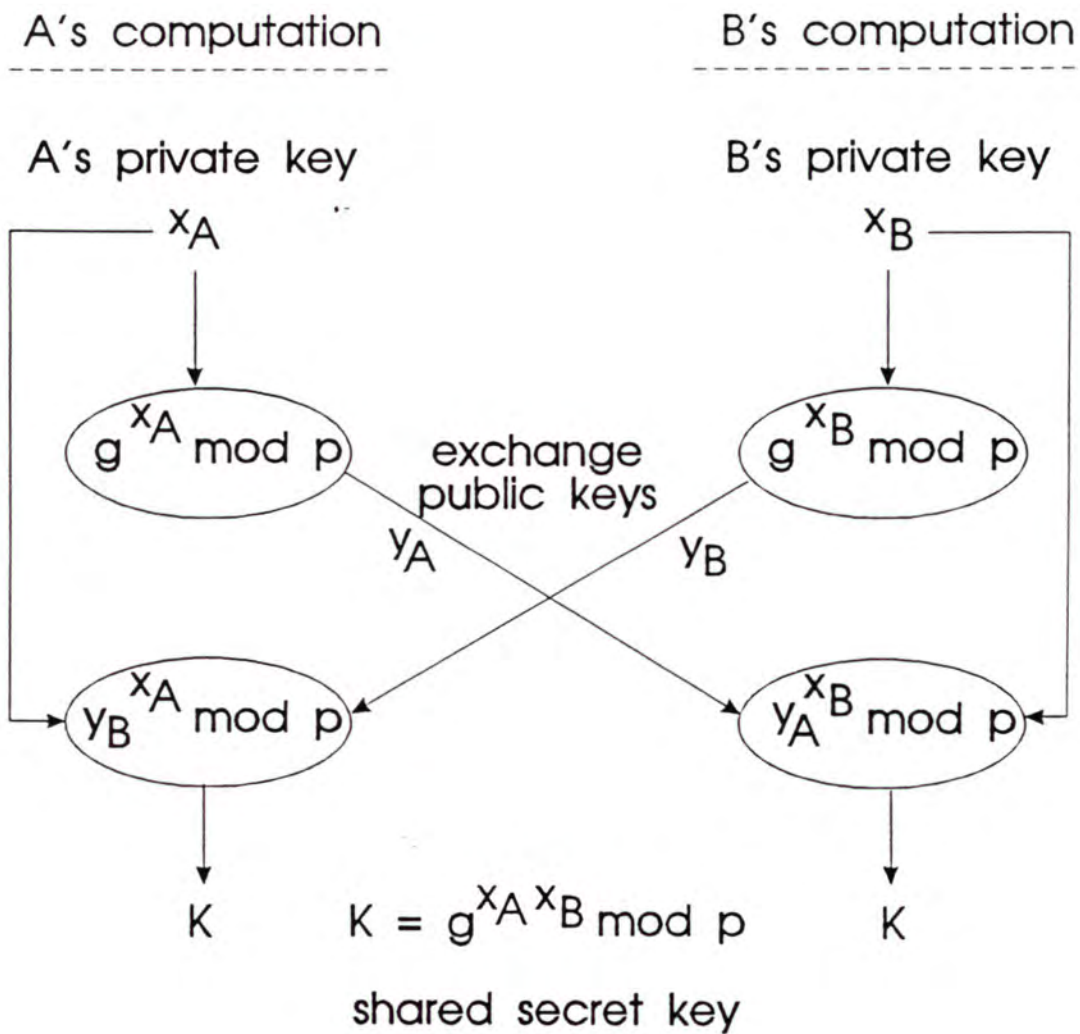


Figure 7. Diffie-Hellman Key Exchange.

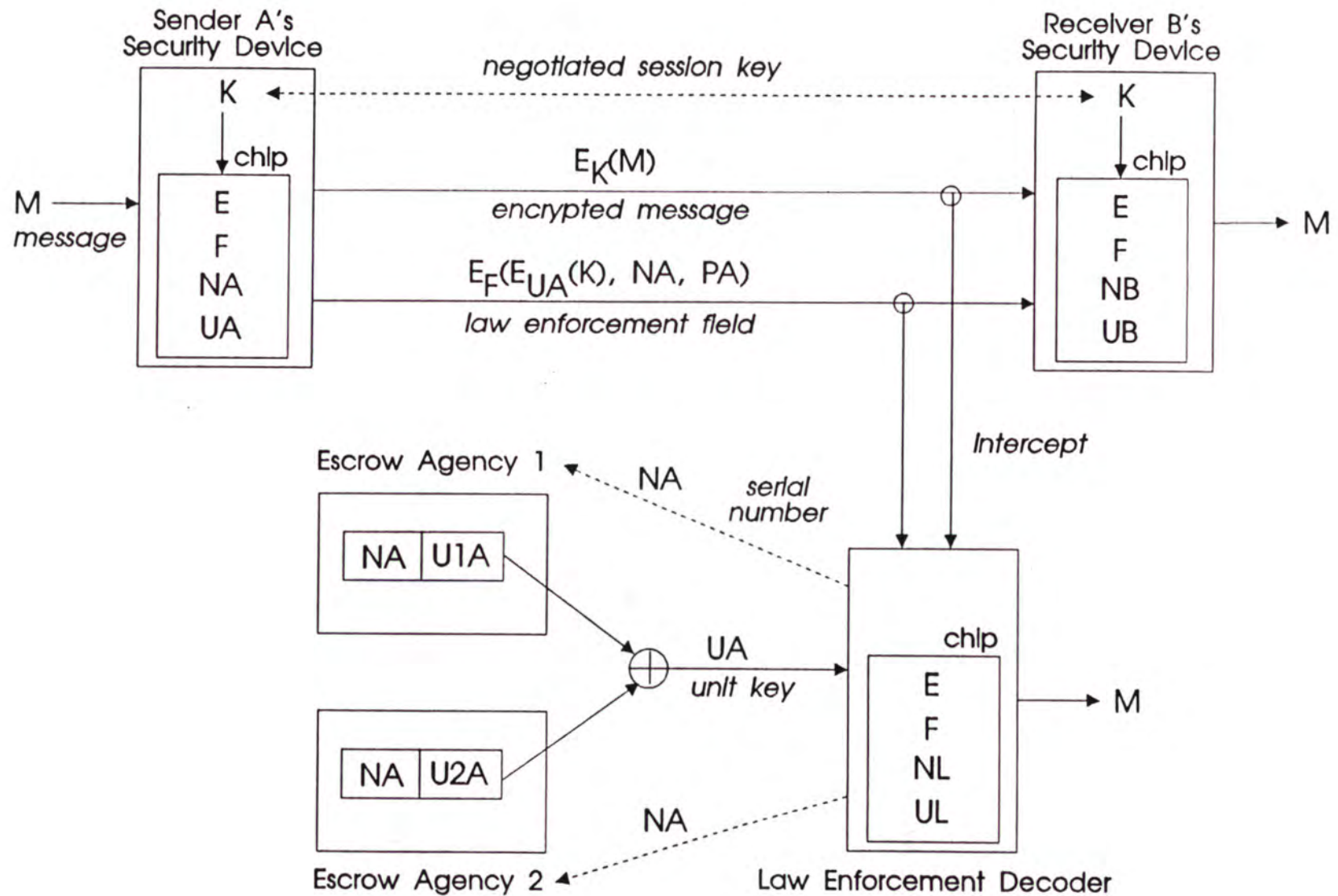


Figure 8. Secure Communications with Law Enforcement Access.

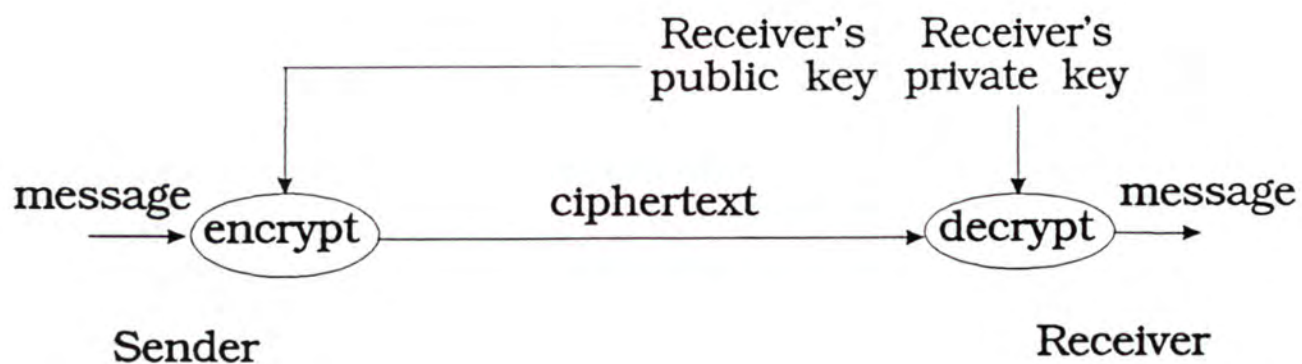


Figure 9. Public-Key Cryptosystem.

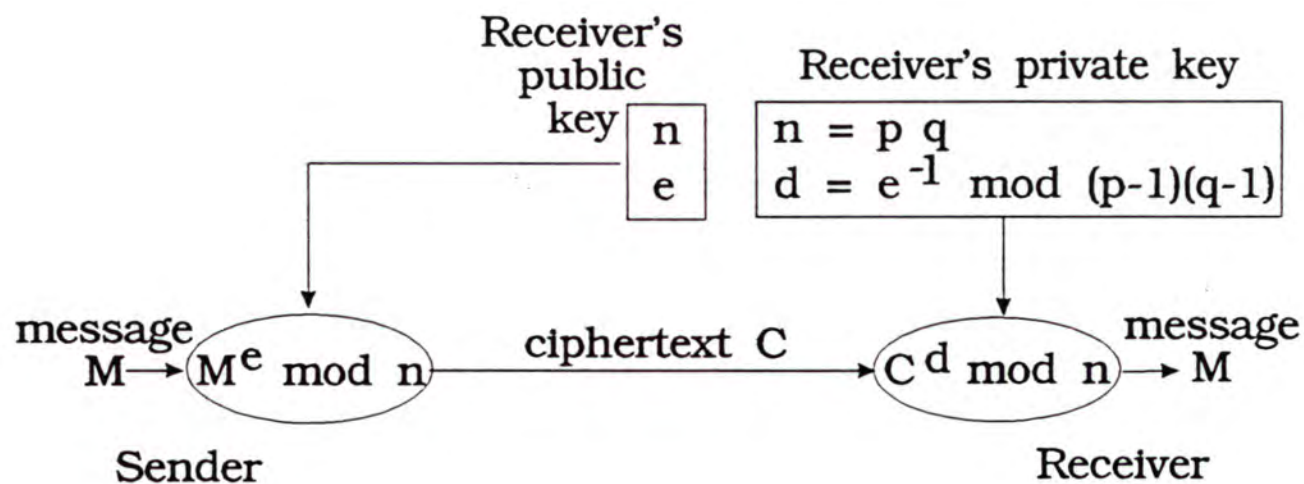


Figure 10. RSA Public-Key Cryptosystem.

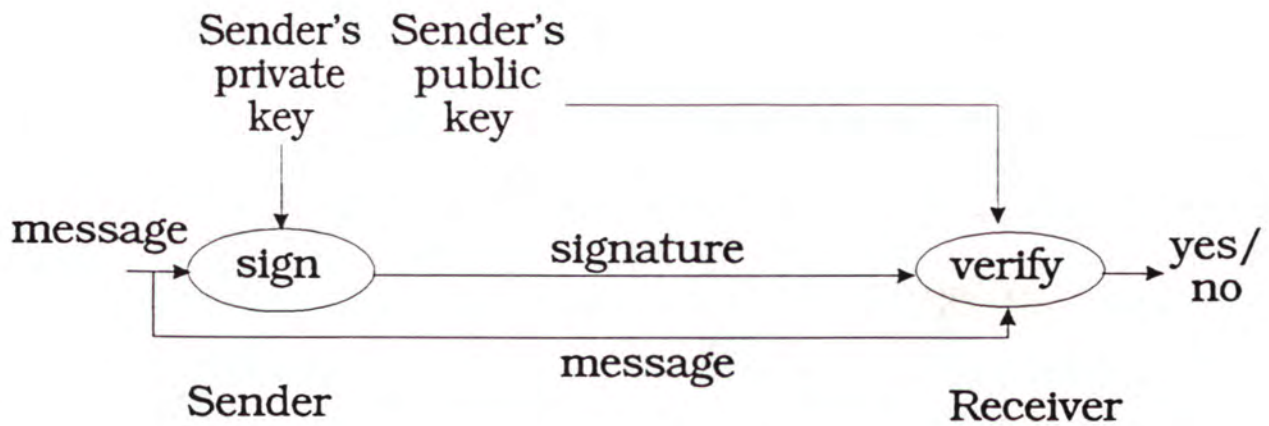


Figure 11. Public-Key Signature System.

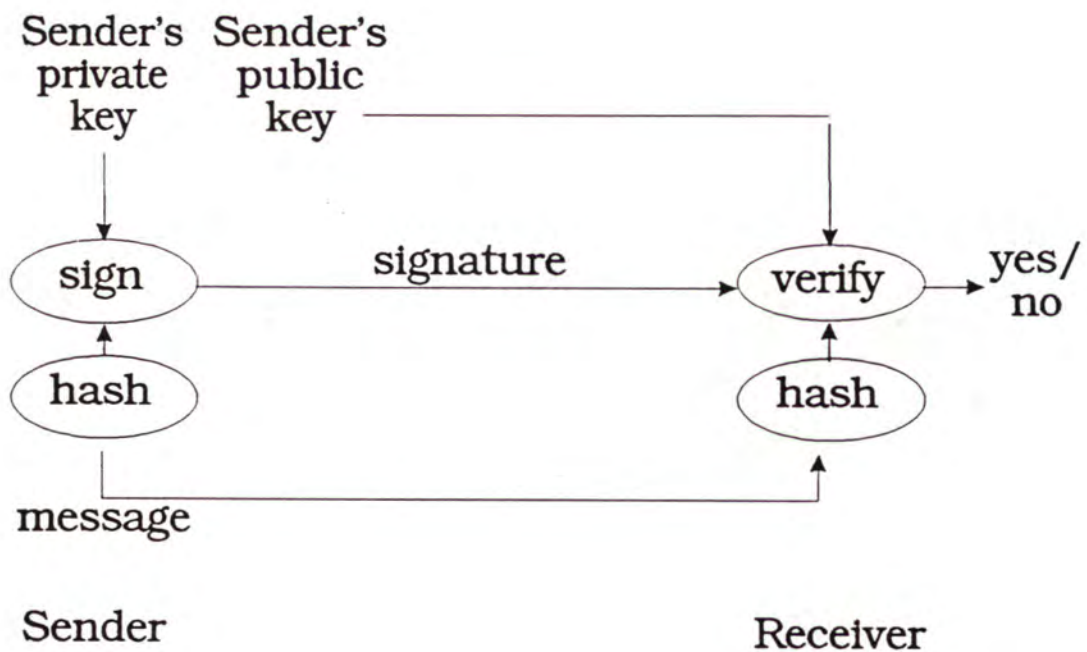


Figure 12. Public-Key Signature System with Hashing.

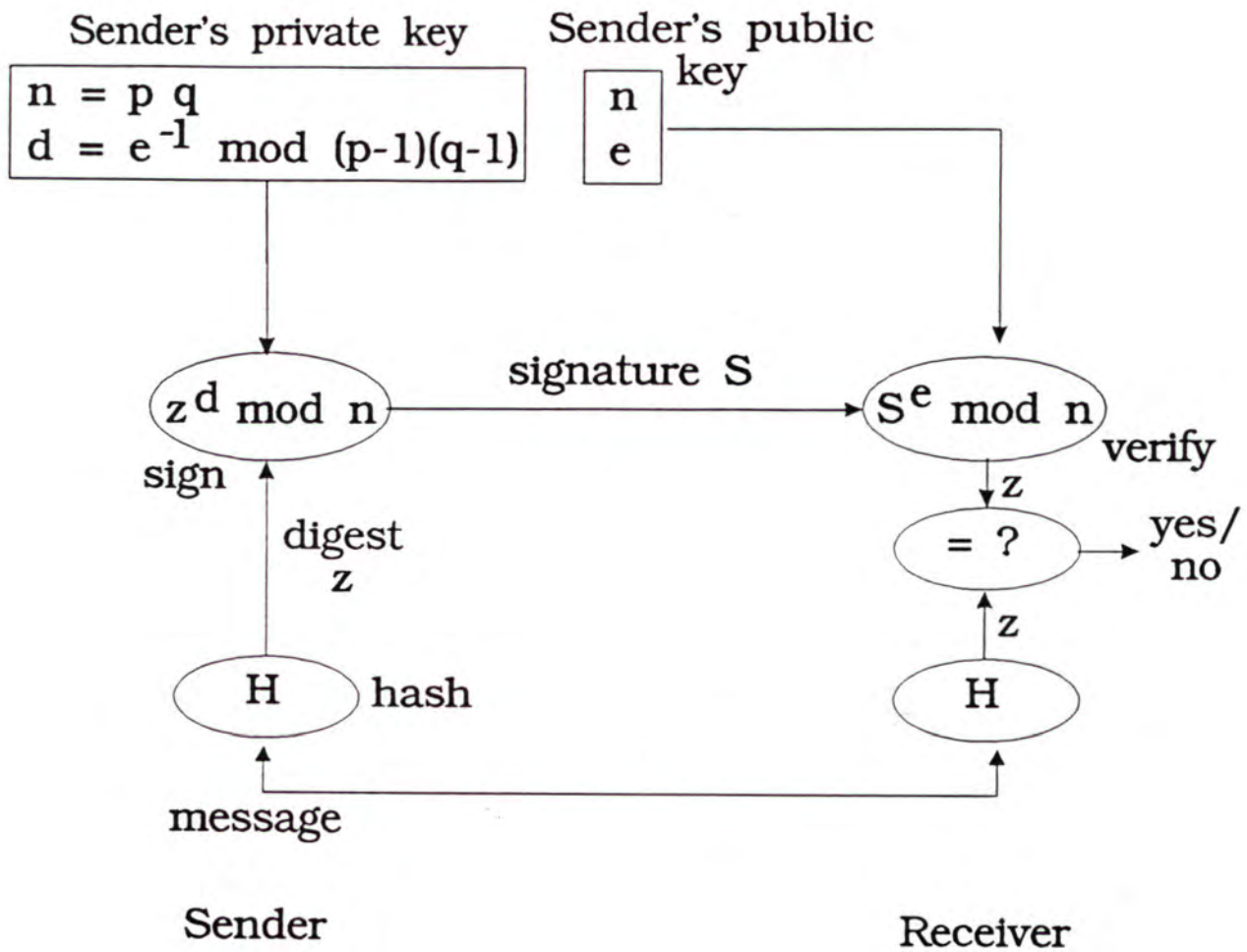


Figure 13. RSA Signature System.

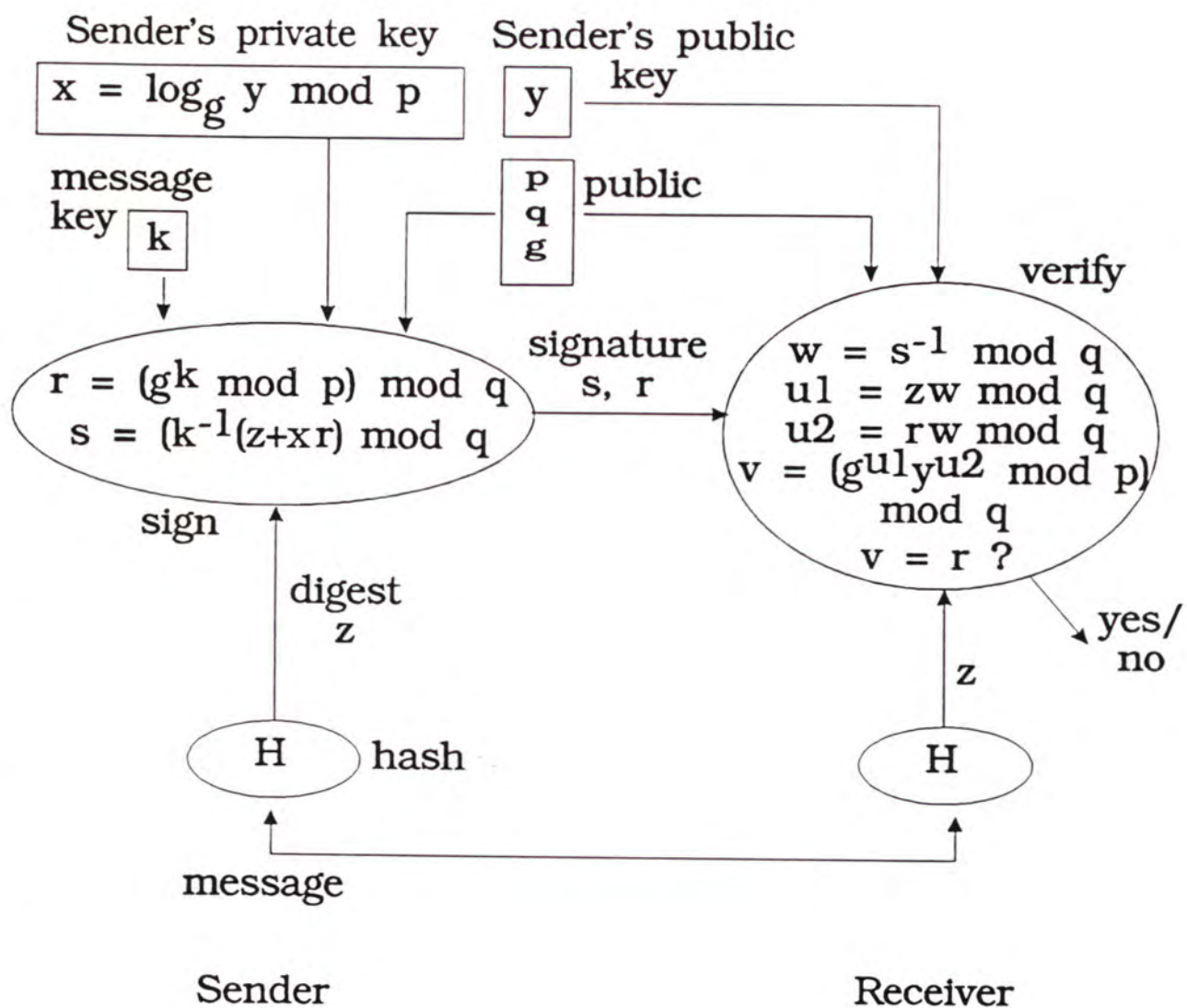


Figure 14. Digital Signature Standard (DSS).