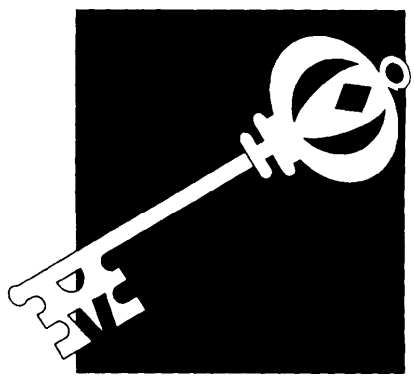
# Government Policies and Cryptographic Safeguards

4

The federal government faces fundamental tension between two important policy objectives: 1 ) fostering the development and widespread use of cost-effective information safeguards, and 2) controlling the proliferation of safeguard technologies that can impair U.S. signals-intelligence and law-enforcement capabilities. This tension runs throughout the government's activities as a developer, user, and regulator of safeguard technologies. The first section of this chapter introduces this tension as it concerns the proliferation of cryp*tography* that could impair U.S. signals intelligence and law enforcement, and the resulting struggle to control cryptography through federal standards and export controls (see box 4-1 ).

The chapter then discusses the effects of governmental concerns about cryptography on the availability and use of safeguards in the private and public sectors. Government agencies differ from most of the private sector in that the impact of national-security concerns on agencies' operational choices is more direct. [1] Agencies must operate according to information-security statutes, executive orders, regulations, policies, guidelines, and



[1] Federal policy for communication security has traditionally been dominated by national security interests, With the convergence of computer and communication technologies, national security concerns have continued to play a major role in information security and the Department of Defense (DOD) and the National Security Agency (NSA) have continued to play the major role in technology and policy development. For an overview of previous federal policy attempts to balance national-security and other interests (embodied in the respective roles of the Departments of Defense and Commerce in developing safeguard standards for civilian agencies), see U.S. Congress, Office of Technology Assessment, *Defending Secrets, Sharing Data: New Locks and Keys for Electronic Information*, OTA-CIT-310 (Washington, DC: U.S. Government Printing Office, October 1987), especially ch. 4 and ch. 6.

## BOX 4-1: What Is Cryptography?

During the long history of paper-based "information systems" for commerce and communication, a number of safeguards were developed to ensure the confidentiality (i e , secrecy of the contents), integrity[1] (i e , without transmission errors or unauthorized changes) and authenticity (i e , coming from the stated source and not forged) of documents and messages These traditional safeguards included secret codebooks and passwords, physical "seals" to authenticate signatures, and auditable bookkeeping procedures Mathematical analogues of these are implemented in the electronic environment. The most powerful of these are based on cryptography. (See "A Note on Terminology, " below. )

The recorded history of cryptography is more than 4,000 years old Manual encryption methods using codebooks, letter and number substitutions, and transpositions have been used for hundreds of years—for example, the Library of Congress has letters from Thomas Jefferson to James Madison containing encrypted passages. Modern, computer-based cryptography and cryptanalysts began in the World War II era, with the successful Allied computational efforts to break the ciphers generated by the German Enigma machines, and with the British Colossus computing machines used to analyze a crucial cipher used in the most sensitive German teletype messages [2]

In the post-WWll era, the premiere locus of U S. cryptographic research and (especially) research in cryptanalysts has been the Department of Defense's National Security Agency (NSA). [3] NSA's preeminent position results from its extensive role in U.S. signals Intelligence and in securing classified communications, and the resulting need to understand cryptography as a tool to protect information and as a tool used by adversaries

Cryptography provides confidentiality through *encoding,* in which an arbitrary table is used to translate the text or message into its coded form, or through *encipherment,* in which an *encryption* algorithm and key are used to transform the original plaintext into the encrypted ciphertext. The original text or message is recovered from the encrypted message through the inverse operation of *decryption—i* e , decoding or deciphering the encrypted message. *Cryptanalysis* is the study and development of various "codebreaking" methods to deduce the contents of the original plaintext message The strength of an encryption algorithm IS a function of the number of steps, storage, and time required to break the cipher and read any encrypted message, without prior knowledge of the key Mathematical advances, advances in cryptanalysts, and advances in computing, all can reduce the security afforded by a cryptosystem that was previously considered "unbreakable" in practice

---

[1] Robert Courtney and Willis Ware have proposed a somewhat different definition of integrity, in terms of "having quality meet a priori expectations " (Willis Ware, personal communication, Apr 29, 1994, *Computers& Security,* forthcoming, 1994)

[2] See Glenn Zorpette, "Breaking the Enemy's Code, " */EEE Spectrum,* September 1987, pp 47-51 More generally, see David Kahn, *The Codebreakers* (New York, NY MacMillan, 1987)

3 For national-security reasons, NSA has a history of efforts to control independent cryptographic research and publication Academic and commercial resistance to NSA's controls increased through the 1970s and 1980s, and sophisticated cryptography of nongovernmental origin began to be offered commercially in the 1980s Notable among these are public-key cryptosystemsthat can be used for confidentiality, authentication, and digital signatures.

*(continued)*

standards that have been established within the framework of national-security concerns. Regarding safeguards based on cryptography, national-security concerns shape the standards available to agencies for use in safeguarding unclassified information. Therefore, these concerns also affect civilian agencies that are usually not thought of in conjunction with "national security." The ability of corporations-as well as government agencies—to appropriately safeguard their infor-

## BOX 4-1: What Is Cryptogra

The strength of a modern encryption scheme is determined by the algorithm itself and the length of the key For a given algorithm, strength Increases with key size. However, key size *alone is* a not a *valid means of comparing the strength of two different encryption systems.* Differences in the properties of the algorithms may mean that a system using a shorter key is stronger overall than one using a longer key

Applications of cryptography have evolved along with cryptographic techniques Cryptography was originally used to protect the confidentiality of communications, encryption is now also used to protect the confidentiality of Information stored in electronic form and to protect the Integrity and authenticity of both transmitted and stored information [4] With the advent of "public-key" techniques, cryptography came into use for "digital signatures" that are of widespread Interest as a means for electronically authenticating and signing commercial transactions like purchase orders, tax returns, and funds transfers, as well as ensuring that unauthorized changes or errors are detected (See below and also discussion of electronic commerce in chapter 3 ) *Thus, cryptography in its modem setting is a technology of broad application.*

Key management is fundamental and crucial to the security afforded by any cryptography-based safeguard Key management Includes generation of the encryption key or keys, as well as their storage, distribution, cataloging, and eventual destruction If secret keys are not closely held, the result is the same as if a physical key is left "lying around" to be stolen or duplicated without the owner's knowledge Similarly, poorly chosen keys may offer no more security than a lock that can be opened with a hairpin Changing keys frequently can limit the amount of information or the number of transactions compromised due to unauthorized access to a given key Thus, a well-thought-out and secure key-management Infrastructure is necessary for effective use of encryption-based safeguards in network environments (See discussion of key infrastructures in chapter 2 )

### A Note on Terminology

Cryptography, a field of applied mathematics/computer science, is the technique of concealing the contents of a message by a code or a cipher A code uses an arbitrary table (codebook) to translate from the message to its coded form, a cipher applies an algorithm to the message

Cryptographic *algorithms—specific* techniques for transforming the original input into a form that is unintelligible without special knowledge of some secret (closely held) information—are used to *encrypt* and decrypt messages, data, or other text The encrypted text is often referred to as *ciphertext,* the original or decrypted text is often referred to as *plaintext* or *cleartext.* In modern cryptography, the secret information is the cryptographic key that "unlocks" the ciphertext and reveals the plaintext

The encryption algorithms and key or keys are Implemented in a *cryptosystem* The key used to decrypt can be the same as the one used to encrypt the original plaintext, or the encryption and decryption keys can be different (but mathematically related) One key is used for both encryption and decryption in *symmetric, or* "conventional" cryptosystems; in *asymmetric,* or "public-key" cryptosystems, the encryption and decryption keys are different and one of them can be made public

[4] Integrity and authenticity are both aspects of a cryptographic safeguard technique called "authentication" or "message authentication (See box 4-4 on digital signatures )

[5] For a glossary see D W Davies and W L Price, *Security for Computer Networks,* 2nd Ed (New York, Ny John Wiley & Sons, 1992)

SOURCE Off Ice of Technology Assessment, 1994, and cited sources


THE NATIONAL CRYPTOLOGIC MUSEUM, NATIONAL SECURITY AGENCY

German *Enigma* cipher machines used during World War II

mation also furthers national security,[2] but (except for government contractors) corporations' technology choices are usually less directly related to the national-security objectives of the governments

Next, the chapter reviews the policy framework within which federal agencies carry out their information security and privacy activities. (Privacy issues and the Privacy Act of 1974 were discussed in chapter 3.) Special attention is given to the Computer Security Act of 1987 (Public Law 100-235) and the responsibilities of the National Institute of Standards and Technology (NIST) and the National Security Agency (NSA) according to the Computer Security Act. These are important in understanding issues related to the develop-

[2]See, e.g., U.S. Congress, House of Representatives, Subcommittee on Economic and Commercial Law, Committee on the Judiciary, *The Threat of Foreign Economic Espionage to U.S. Corporations*, hearings, 102d Cong., 2d sess., Apr. 29 and May 7, 1992, Serial No. 65 (Washington, DC: U.S. Government Printing Office, 1992).

[3]Federal Information Processing Standards (FIPS) usually apply to agencies and their contractors. Sometimes they are incorporated into voluntary industry and or international standards, in which case they do help shape technology choices in the private sector.

ment and use of federal safeguard standards and guidelines. Some of these Federal Information Processing Standards (FIPS) have been incorporated in industry and international standards.

The chapter looks at two major mechanisms the government uses to control cryptography: *export controls* and *standards setting. The* current activities of NIST and NSA regarding information safeguards and standards are reviewed. Two recent FIPS, the Digital Signature Standard (DSS) and the Escrowed Encryption Standard (EES), are examined in terms of a long-term government strategy to control the availability and use of information safeguards based on cryptography.

The final section of this chapter presents policy options for congressional consideration. These include near-term options related to cryptography policy (including export controls and federal standards based on cryptography), as well as strategic options for a broad congressional review of national cryptography policy.

## IMPORTANCE OF CRYPTOGRAPHY

The tension between promoting and controlling the widespread use of safeguards has existed for decades, but changes in the international arena, in technology, and in the needs of user communities (e.g., as in the Internet) are bringing it to the forefront of public attention.[4] This tension is manifested in export controls on a fundamental technology for safeguarding information--cryptography--and in the federal government's process for developing and promulgating cryptography-based standards for use in safeguarding unclassified information.

From the end of World War I through the mid- 1970s, the federal government was almost the sole source of technology and know-how for safeguards that used cryptography to ensure information confidentiality. This monopoly has been eroding, however. Good encryption technology is available commercially in the United States and abroad, and cryptography research is international. These developments have raised questions-especially from software developers—as to whether existing policies concerning the sale and export of encryption products are outdated and should be modified, or whether continued restrictions are still required to meet national- security and signals-intelligence objectives.[5] These topics are discussed later in this chapter, with a focus on government operations and attempts to balance national-security and other objectives, like personal rights, open government, and market competitiveness; their impact on the safeguards marketplace in general is discussed in chapter 2.

Policy debate in this area used to be almost as arcane as the technology itself. Most people didn't regard government decisions about cryptography as having direct effect on their lives. However, the technology of daily life is changing, making electronic transactions and records central to everything from commerce to health care. Thus, concern over the implications of privacy and security policies dominated by national-security objectives has grown dramatically in business and academic communities that produce or use information safeguards, as well as among the general public (see chapter 3).[6] This concern is evidenced in the debates over the government's

[4] For example, good safeguards are needed to protect U.S. information from foreign intelligence, but the same safeguards might be used to protect foreign communications from U.S. intelligence. A similar argument can be made from a law-enforcement perspective.

[5] Commercial security products containing robust cryptography that can be used for confidentiality --i.e., that can do strong encryption— are subject to strict export controls and usually cannot be exported, except for limited applications like banking. Thus, when international interoperability is desired, export controls form a barrier to use of many U.S.-origin encryption products (including software products) in security systems. However, the same technologies are often readily available outside the United States. See discussion of export controls later in this chapter.

[6] See Susan Landau et al., *Codes, Keys, and Conflicts: Issues in U.S. Crypto Policy,* report of a special panel of the ACM U.S. Public Policy Committee (New York, NY: Association for Computing Machinery, June 1994).

Escrowed Encryption Standard, colloquially referred to as *Clipper* or the *Clipper chip. The* EES is intended for use in safeguarding voice, facsimile, or computer data communicated in a telephone system7 (see box 4-2).

Previously, control of the availability and use of cryptography was presented as a national-security issue focused outward, with the intention of maintaining a U.S. technological lead, compared with other countries. Now, with an increasing domestic policy focus on crime and terrorism, the availability and use of cryptography has also come into prominence as a domestic-security, law-enforcement issue. More widespread foreign use of cryptography-including use by terrorists and developing countries—makes U.S. signals intelligence more difficult. Within the United States, cryptography is increasingly being portrayed as a threat to domestic security (public safety) and a barrier to law enforcement if it is readily available for use by terrorists or criminals.[8] There is also growing recognition of the potential misuses of cryptography, such as by disgruntled employees as a means to sabotage an employer's databases.[9]

In May 1994 testimony before the Subcommittee on Technology, Environment, and Aviation of the House Committee on Science, Space, and Technology, James Kallstrom of the Federal Bureau of Investigation (FBI) noted:

> [The Omnibus Crime Control and Safe Streets Act of 1968] permits electronic surveillance only for serious felony offenses and only when other investigative techniques will not work or are too dangerous. Since 1968, law enforcement has used this crime-solving and crime-preventing technique very effectively and judiciously to protect our people. In a ten-year period ending in 1992, more than 22,000 convictions have resulted from court-authorized surveillances .'"
>
> . . . the use of excellent cryptographic products by the myriad array of criminals and terrorists poses an extremely serious threat to the public safety and national security.

---

[7] The Clipper chip is designed for use in telephone systems; it contains the EES encryption algorithm, called *SKIPJACK. The* Capstone chip and TESSERA PCMCIA card also contain the SKIPJACK algorithm; these implementations are for use in data communications. (Clinton Brooks, Special Assistant to the Director, NSA, personal communication, May 25, 1994.)

The Clipper chip is being used in the AT&T Surity Telephone Device 3600, which has a retail price of about $1,100. It has been approved for government use for unclassified voice encryption. The Department of Justice purchased 9,000 of them. AT&T sells another version of the Surity 3600, using a proprietary AT&T encryption algorithm, for about the same price. (Brad Bass, "AT&T Unveils First Clipper Device on GSA Schedule," *Federal Computer Week,* May 9, 1994, pp. *24,29.)*

*8* For example, high. quality, low-cost voice encryptors are becoming available at reasonable cost. For recent exposition of law-enforcement and national-security concerns with respect to cryptography and the rationale for the EES, see Jo Ann Hams, Assistant Attorney General, Criminal Division, U.S. Department of Justice, testimony presented before the Subcommittee on Technology and the Law, Committee on the Judiciary, U.S. Senate, May 3, 1994; Vice Adm. J.M. McConnell, Director, National Security Agency, testimony presented before the Subcommittee on Technology and the Law, Committee on the Judiciary, U.S. Senate, May 3, 1994; and James K. Kallstrom, Special Agent in Charge, Special Operations Division, New York Field Division, Federal Bureau of Investigation, testimony presented before the Subcommittee on Technology, Environment and Aviation, Committee on Science, Space and Technology, U.S. House of Representatives, May 3, 1994.

See also Landau et al., op. cit., footnote 6; and Dorothy E. Denning, "The U.S. Key Escrow Encryption Technology," in *Computer Communications* (Oxford, UK: Butterworth-Heinemann Ltd., in press). But see David Banisar, "Roadblocks on the Information Superhighway: Governmental Intrusions on Privacy and Security," *Federal Bar News and Journal,* in press.

[9] See Dorm B. Parker, Senior Management Consultant, SRI International, "Crypto and Avoidance of Business Information Anarchy," September 1993 (obtained from the author). Parker describes problems that could occur in organizations if cryptography is used without adequate key management and override capabilities by responsible corporate officers. These problems include keys being held for ransom by disgruntled employees, data being rendered inaccessible after being encrypted by employees who then leave to start their own company, and so forth.

[10] Kallstrom testimony, op. cit., footnote 8, p. 3. Kallstrom noted that in 1992 the total number of criminal wiretap orders obtained by all federal, state, and local law-enforcement agencies was 919; about two-thirds of these were for serious state and local felonies.

## BOX 4-2: What Is the EES?

The federal Escrowed Encryption Standard (EES) was approved by the Department of Commerce as a Federal Information Processing Standard (FIPS) in February 1994.[1] According to the standard (see FIPS Publication 185), the EES is intended for voluntary use by all federal departments and agencies and their contractors to protect unclassified Information. Implementations of the EES are subject to State Department export controls However, encryption products based on EES may be exported to most end users, and these products will qualify for special licensing arrangements [2]

The EES is Intended to encrypt voice, facsimile, and computer data communicated in a telephone system It may, on a voluntary basis, be used to replace DES encryption devices now in use by federal agencies and contractors Other use by the private sector is voluntary The EES specifies a symmetric encryption algorithm, called *SKIPJACK.* The SKIPJACK algorithm is a classified algorithm, developed by NSA in the 1980s [3] An early Implementation was called Clipper, hence the colloquial use of Clipper or Clipper chip to describe the EES technology [4]

The EES also specifies a method to create a Law Enforcement Access Field (LEAF), in order to provide for easy decryption when the equivalent of a wiretap has been authorized [5] The SKIPJACK algorithm and LEAF creation method are Implemented only in electronic devices (i e , very-large-scale-integration chips) The chips are "highly resistant" to reverse engineering and will be embedded in tamper-resistant cryptographic modules that approved manufacturers can incorporate in telecommunications or computer equipment The chips are manufactured by VLSI Logic and are programmed with the algorithms and keys by Mykotronx. The programming is done under the supervision of the two "escrow agents" (see below)

After electronic surveillance has been authorized, the EES facilitates law enforcement access to encrypted communications This is accomplished through what is called a "key escrowing" scheme Each EES chip has a chip-specific key that is split into two parts after being programmed into the chips These parts can be recombined to gain access to encrypted communications. One part is held

---

[1] *See Federal Register,* vol 59, Feb 9. 1994, pp 5997-6005 FIPS Publication 185 ("Escrowed Encryption Standard, " 1994) describes the applicability, Implementation, and maintenance of the standard, as well as specifications for its use Unlike the DES algorithm, the EES algorithm is classified and not publicly available for inspection

[2] Martha Harris Deputy Assistant Secretary of State for Political-Military Affairs, "Statement on Encryption-Export Control Reform, Feb 4, 1994

[3] The NSA specification for SKIPJACK is contained in "SKIPJACK, R21 -TECH-044-01 ," May 21, 1991, this technical report is classified at the Secret level The NSA specifications for the LEAF creation method are contained in "Law Enforcement Access Field for the Key Escrow Microcircuit, " also classified at the Secret level Organizations holding an appropriate security clearance and entering into a Memorandum of Agreement with NSA regarding Implementation of the standard can have access to these (OTA project staff did not access these, or any other classified information in the course of this study)

[4] The Clipper chip implementation of SKIPJACK is for use in secure telephone communications An enhanced escrowed-encryption chip with more functions, called Capstone, is used in data communications

[5] See Jo Ann Harris, Assistant Attorney General, Criminal Division, Department of Justice, testimony before the Subcommittee on Technology and the Law, Committee on the Judiciary, U S Senate, May 3, 1994, and James K Kallstrom, Special Agent in Charge, Special Operations Demon, Federal Bureau of Investigation, testimony before the Subcommittee on Technology, Environment, and Aviation, Committee on Science, Space, and Technology, U S House of Representatives, May 3, 1994 For a discussion of law enforcement concerns and the rationale for government key escrowing, see also Dorothy E Denning, "The Clipper Encryption System" *American Scientist* vol 81, July-August 1993, pp 319-322, and "Encryption and Law Enforcement," Feb 21, 1994, available from denning@cs georgetown edu

*(continued)*

## BOX 4-2 (cont'd.): What Is the EES?

by each of two designated government keyholders, or "escrow agents, " When surveillance has been authorized and the intercepted communications are found to be encrypted using the EES, law enforcement agencies can obtain the two parts of the escrowed key from the escrow agents, These parts can then be used to obtain the individual keys used to encrypt (and, thus, to decrypt) the telecommunications sessions of interest.[6] The LEAF is transmitted along with the encrypted message; it contains a device identifier that indicates which escrowed keys are needed. (A more technical description of how the EES IS said to work is in chapter 2.)

The National Security Council, Justice Department, Commerce Department, and other federal agencies were involved in the decision to propose the EES according to a White House press release and information packet dated April 16, 1993, the day the EES initiative was announced. The EES algorithm is said to be stronger than the Data Encryption Standard (DES) algorithm, but able to meet the legitimate needs of law enforcement agencies to protect against terrorists, drug dealers, and organized crime [7]

Attorney General Reno designated the National Institute of Standards and Technology and the Treasury Department's Automated Systems Division as the original escrow agents NIST's first estimate of the costs of establishing the escrow system was about $14 million, with estimated annual operating costs of $16 million. Cost figures and escrowing procedures are being refined by the Clinton Administration NIST did not provide the OTA with more precise estimates of the resources, including staff, required to implement and manage key escrowing.

The proposed FIPS was announced in the *Federal Register* on July 30, 1993 and was also sent to federal agencies for review. The EES was promulgated after a comment period that generated almost universally negative comments According to NIST, comments were received from 22 government organizations. in the United States, 22 industry organizations, and 276 individuals Concerns and questions reported by NIST include the algorithm itself and lack of public inspection and testing, the role of NSA in promulgating the standard, use of key escrowing, possible infringement of individual rights, effects of the standard on U S firms' competitiveness in foreign markets, cost of establishing the escrowing system, and cost-effectiveness of the new standard [8]

During the review period, the SKIPJACK algorithm was evaluated by outside experts, pursuant to President Clinton's direction that "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 " Five reviewers accepted NIST's invitation to participate in a classified review of SKIPJACK and publicly report their findings Ernest Brickell (Sandia National Laboratories), Dorothy Denning (Georgetown University), Stephen Kent (Bolt Beranek and Newman, Inc. ), David Maher (AT&T), and Walter Tuchman

---

6 Requirements for federal and state law-enforcement agents to certify that electronic surveillance has been authorized, and for what period of time, as well as requirements for authorized use of escrowed key components are explained in Department of Justice, "Authorization Procedures for Release of Encryption Key Components In Conjunction with Intercepts Pursuant to Title III," "Authorization Procedures for Release of Encryption Key Components in Conjunction with Intercepts Pursuant to Slate Statutes," and "Authorization Procedures for Release of Encryption Key Components in Conjunction with Intercepts Pursuant to FISA, " Feb 4, 1994

7 Because the EES algorithm is classified, the overall strength of the EES cannot be examined except under security clearance (see note 9 below) Thus, unclassified, public analyses of its strengths and weaknesses are not possible

The only public statements made by the Administration concerning the strength of the EES relative to the DES refer to the secret key size 80 bits for the EES versus 56 bits for the DES Longer keys offer more protection from exhaustive-search attacks (see box 4-3), but the overall strength of a cryptosystem is a function of both key size and the algorithm itself

8 *Federal Register* ( Feb 9, 1994), op cit fOOtnOte 1, PP 5998-6002

*(continued)*

## BOX 4-2 (cont'd.): What Is the EES?

(Amperif Corp.). Their interim report on the algorithm itself found that: 1) there is no significant risk SthatKIPJACK will be broken by exhaustive search in the next 30 to 40 years; 2) there is no significant risk that SKIPJACK can be broken through a shortcut method of attack; and 3) while the internal structure of SKIPJACK must be classified in order to protect law-enforcement and national-security objectives, the strength of SKIPJACK against a cryptanalytic attack does not depend on the secrecy of the algorithm.[9] The reviewers will issue a final report on broader system issues in implementing SKIPJACK.

Based on its review of the public comments, NIST recommended that the Secretary of Commerce issue the EES as a Federal Information Processing Standard.[10] NIST noted that almost all of the comments received during the review period were negative, but concluded that, "many of these comments reflected misunderstanding or skepticism that the EES would be a *voluntary* standard."[11] The Clinton Administration also carried out a 10-month encryption policy review that presumably played a role in choosing to issue the EES as a FIPS, but the substance of that review has not been made public and was not available to OTA. Additionally, the Clinton Administration created an interagency working group on encryption and telecommunications that includes representatives of agencies that participated in the policy review. The working group will be chaired by the Office of Science and Technology Policy and the National Security Council and will "work with industry on technologies like the Key Escrow chip [i.e., the EES], to evaluate possible alternatives to the chip, and to review Administration policies regarding encryption as developments warrant."[12]

9 E Brickell (Sandia National Laboratories) et al "SKIPJACK Review Interim Report—The SKIPJACK Algorithm," July 28.1993
See also "Fact Sheet—NIST Cryptography Activities," Feb 4, 1994
10 Ibid and *Federal Register* (Feb 9, 1994), Op cit, footnote 1
11 Ibid
12 White House press release and enclosures, Feb 4, 1994, "Working Group on Encryption and Telecommunications"

SOURCE Off Ice of Technology Assessment, 1994 and references cited below

The essence of the cryptographic threat is that high-grade and user-friendly encryption products can seriously hinder law enforcement and counterintelligence agencies in their ability to conduct electronic surveillance that is often necessary to carrying out their statutorily-based missions and responsibilities. In particular, some encryption products put at risk efforts by federal, state and local law enforcement agencies to obtain to [sic] contents of intercepted communications by precluding real-time decryption. Real-time decryption is often essential so that law enforcement can rapidly respond to criminal activity and, in many instances, prevent serious and life-threatening criminal acts.[11]

Expressing support for the EES and key-escrowing initiatives, Kallstrom stated that:

> We fully support the Vice President's initiative to create a national information superhighway to share information, educate Americans, and increase productivity. However, it would be wrong for us as public servants to knowingly allow this information superhighway to jeopardize the safety and economic well-being of law-abiding Americans by becoming an expressway and safe haven for terrorists, spies, drug dealers, and murderers.[12]

Thus, export controls, intended to restrict the international availability of U.S. cryptography technology and products, are now being joined by

11 Ibid., p. 12.

12 Ibid., p. 14.

domestic initiatives that offer alternative cryptography-based technologies for safeguarding unclassified information. These initiatives are intended to preserve U.S. law-enforcement and signals-intelligence capabilities. According to NIST Deputy Director Raymond Kammer:

> In developing cryptographic standards, one can not avoid two often competing interests. On the one hand are the needs of users-corporate, government, and individual—in protecting telecommunications transmissions of sensitive information. . . On the other hand are the interests of the national security and law enforcement communities in being able to monitor electronic communications. In particular, I am focusing upon their need for continued ability to keep our society safe and our nation secure.
>
> Rapid advances in digital telecommunications have brought this issue to a head. Some experts have stated that, within ten years, most digital telecommunications will be encrypted. Unless we address this issue expeditiously, law enforcement will lose an important tool in fighting crime—the ability to wiretap-and the mission of our Intelligence Community will be made more difficult. [13]

The EES has been promulgated by the Clinton Administration as a voluntary alternative to the current federal encryption standard used to safeguard unclassified information, the Data Encryption Standard (DES). [14] The symmetric encryption algorithm used in the DES is now over 20 years old; this standard allows users to generate their own encryption keys and does not require the keys to be deposited with any third party. [15] The DES algorithm has been made public (i.e., it has been published) and can be freely implemented in hardware or software (see box 4-3).

The algorithm specified in the Escrowed Encryption Standard has not been published. It is classified and the algorithm is intended to be implemented only in tamper-resistant, hardware

---

[13] Raymond G. Kammer, NIST Deputy Director, testimony presented before the Subcommittee on Technology and the Law, Committee on the Judiciary, U.S. Senate, May 3, 1994, p. 2. NIST is responsible for developing the FIPS for protecting information in unclassified computer systems.

[14] NIST, "Data Encryption Standard (DES)," FIPS PUB 46-2 (Gaithersburg, MD: U.S. Department of Commerce, Dec. 30, 1993).

An alternative successor to the DES is *triple-encryption DES*, where the algorithm is used sequentially with three different keys, to encrypt, decrypt, then re-encrypt. There is, however, no FIPS for triple-encryption DES. Triple encryption with the DES offers more security than having a 112-bit key and, therefore, appears inviolate against all adversaries for the foreseeable future. (Martin Hellman, Professor of Electrical Engineering, Stanford University, personal communication, May 24, 1994; also see box 4-3.)

[15] As with other encryption techniques, sound key management (i.e., key generation and protection, key distribution and destruction) is vital to the overall security of the system. See NIST, "Guidelines for Implementing and Using the NBS Data Encryption Standard," FIPS PUB 74 (Gaithersburg, MD: U.S. Department of Commerce, Apr. 1, 1981); and "Key Management Using ANSI X9.1 7," FIPS PUB 171 (Gaithersburg, MD: U.S. Department of Commerce, Apr. 27, 1992).

## BOX 4-3: What Is the DES?

The Data Encryption Standard (DES) is a published, federal encryption standard for use in protecting unclassified computer data and communications. It has also been incorporated in numerous industry and international standards. The DES was promulgated by the Commerce Department, under authority of the Brooks Act of 1965 (Public Law 89-306). The Secretary of Commerce first approved the DES as a Federal Information Processing Standard (FIPS) in November 1976; it was published as FIPS Publication 46 ("Data Encryption Standard") in January 1977 and became effective in July 1977.

The encryption algorithm specified by the DES is a symmetric, *secret-key algorithm* called the Data Encryption Algorithm (DEA). The DES algorithm uses a 64-bit key; eight bits are used only for parity checking, so the actual "secret key" is 56 bits long. The DES can be used in four standard modes of operation; these vary in their characteristics, strengths, and error-propagation properties, and are specified in FIPS Publication 81 ("DES Modes of Operation," 1980). The DES can be used in message authentication; use of the DES in the Data Authentication Algorithm is specified in FIPS Publication 113 ("Computer Data Authentication," 1985). Message authentication (e.g., of electronic funds transfers) using the DEA is standard in banking and the financial community. Using Merkle's "tree-signature" technique, the DES can be used to generate digital signatures, but in general it is more efficient and convenient to use a public-key system for signatures.[1]

The DES was promulgated with the provision that it be reviewed for continued suitability at five-year intervals and that it would be reaffirmed (or not) for use by federal agencies every five years. The DES was reaffirmed for the first time in 1983. By 1986, over 400 models of voice, data, and file encryption products had been tested and endorsed by the National Security Agency as meeting the standard specifications. (At that time, software implementations of the DES were not certified for government use but were widely used in the private sector, so the total number of DES-based products was much larger.) Vendor and user communities were thrown into an uproar in 1986, when NSA announced it would terminate endorsement of DES products in 1988, in favor of a new set of incompatible, classified, hardware standards that were developed by NSA and were said by the agency to offer more security.[2] The banking community was particularly concerned with the prospect of having to replace the DES with the NSA technology, particularly after having invested heavily in DES-based systems. Ultimately, however, the DES was reaffirmed in 1988, following passage of the Computer Security Act of 1987. The National Institute of Standards and Technology validates DES implementations that meet the standard.

The DES was reaffirmed again this time in software as well as hardware and firmware implementations in December 1993 as FIPS Publication 46-2. *This is likely to be the last time it is reaffirmed as a federal standard.* FIPS Publication 46-2 notes that the algorithm will be reviewed within five years to assess its adequacy against potential new threats, including advances in computing and cryptanalysis: "At the next review (1998) the [DES algorithm] will be over twenty years old. NIST will consider alternatives which offer a higher level of security. One of these alternatives may be proposed as a replacement standard at the 1998 review" (p. 6). An alternative that is currently favored by the "public" cryptography community (i.e., in the private sector and academia) is triply encrypted DES (see below).

---

[1] See box 4-4 for discussion of digital signatures. Ralph Merkles "tree signature techniques" made the use of symmetric (secret key) ciphers like the DES more usable for digital signatures. However, asymmetric cryptography is still preferred for digital signatures (Martin Hellman, Professor of Electrical Engineering, Stanford University, personal communication, Apr. 24, 1994, and Burton Kaliski, Jr., Chief Scientist, RSA Laboratories, personal communication, Apr. 20, 1994.)

[2] The Commercial Communications Security Endorsement Program (CCEP) was an NSA-industry program to develop the embeddable cryptographic modules; host products for the modules were developed under an NSA-industry program called the Development Center for Embedded COMSEC Products (DCECP).

*(continued)*

## BOX 4-3 (cont'd.): What Is the DES?

Controversy surrounded NSA's role in the selection and refinement of the encryption algorithm that was promulgated as the DES In 1973, the National Bureau of Standards (now NIST) had issued a solicitation for candidate algorithms for a federal encryption standard, but received no suitable candidates A year later, IBM responded to a second NBS solicitation with what eventually became the DES, The original algorithm developed by IBM, using a longer key, had been submitted to NSA for classification review as part of the patenting process NSA chose not to classify the algorithm and suggested that IBM submit it—but with some modification—to NBS for consideration as the standard, NBS eventually promulgated the modified IBM algorithm as the DES algorithm.[3]

The modifications suggested by NSA and made by IBM gave rise to concerns that NSA had deliberately weakened or "tampered with" IBM's algorithm in order to maintain U.S. signals-intelligence capabilities. Although the algorithm was made public, the design criteria used by IBM and the results of NSA's testing and evaluation were not, nor were the design criteria used by NSA that led to shortening the key length and modifying a feature of the algorithm called the *substitution boxes,* or *S-boxes.* After much public debate, an inquiry by Representative Jack Brooks led the Senate Select Committee on intelligence to conduct a classified investigation This investigation concluded that

> In the development of the DES, NSA convinced IBM that a reduced key size was sufficient, indirectly assisted in the development of the S box structures, and certified that the final DES algorithm was, to the best of their knowledge, free of any statistical or mathematical weaknesses. NSA did not tamper with the design of the algorithm in any way. IBM invented it and designed the algorithm, made all pertinent decisions regarding it, and concurred that the agreed on key size was more than adequate for all commercial applications for which the DES was intended [4]

The reason for attention to the key size was that a longer key would have made it much harder to find a particular secret key through an "exhaustive search" cryptanalysts, in which all possible keys are tried in order to find the one being used Because the secret key is 56 bits long, an exhaustive search would, in principle, require $2^{56}$ operations Doubling the key size does far more than double the strength against exhaustive attacks—if the key were 112 bits long, exhaustive search would, in principle, require $2^{112}$ Operations, which is roughly 100,000 million million times as much work.[5]

For a given key size, "multiple encryption" can increase the security of the final ciphertext. The increase depends on the characteristics of the encryption algorithm, with the DES the gain is less than would be achieved through an increase in key size, but can still be adequate That is, encrypting twice with the DES, using two different keys, is nowhere near as secure as having a true 112-bit key The preferred method to strengthen the DES is through *triple encryption.* In this technique, the original plaintext is encrypted using one key; the resulting ciphertext is decrypted using a different second key, the

---

3 For more on the history of the DES and controversy surrounding Its 1988 reaffirmation, see U S Congress, Off Ice of Technology Assessment, *Defending Secrets, Sharing Data New Locks and Keys for Electronic Information,* OTA-CIT-310 (Washington, DC U S Government Printing Office, 1987), especially chapter 4 and appendix C

4 U S Senate, Select Committee on Intelligence, *Unclassified Summary Involvement of NSA m the Development of the Data Encryption Standard (Staff Report),* 95th Cong 2d sess (Washington, DC U S Government Printing Off Ice, April 1978), p 4 See also OTA, op cit , footnote 3, pp 169-171

5 Martin Hellman, op cit , footnote 1

6 See Ralph C Merkle and Martin Hellman, "on the Security of Multiple Encryption, " *Communications of the ACM,* vol 24, No 7, July 1982, pp 465-467

*(continued)*

## BOX 4-3 (cont'd.): What Is the DES?

result is encrypted again, with a third key[6] (The plaintext is recovered by reversing the operations, using all 3 keys) Triple encryption with the DES offers more security than having a 112-bit key and therefore, appears Inviolate against all adversaries for the foreseeable future.[7]

Interestingly, it now appears that the NSA-suggested modifications to the S-boxes were intended to strengthen the algorithm against another, particularly powerful type of attack called differential *cryptanalysis* Eli Biham and Adi Shamir published the first paper on differential cryptanalysts, which they discovered in 1990 After this announcement, a member of the IBM design team stated that the IBM designers—and presumably NSA—knew about it no later than 1974[8]

7 Multiple encryption With the DES offers less of an Increase in security than multiplying the keylength by the same factor because of the way the individual bits of the key are "mixed'" during encryption Triple encryption with DES offers much less of an increase in strength than using a 168-bit (3 X 56 bits) key, but is much stronger than double encryption and is better than using a 1 12-bit key (Martin Hellman, Professor of Electrical Engineering, Stanford University, personal communication, May 10 1994 )

8 Don Coppersmith of IBM as quoted in Bruce Schneier, "A Taxonomy of Encryption Algorithms, " *Computer Security Journal*, vol IX, No 1, pp 39-59 (quote at p 42) See also E Biham and A Shamir, "Differential Cryptanalysts of DES-like Cryptosystems" *Advances m Cryptology,CRYPTO "90 Proceedings (New* York, NY Springer-Verlag, 1991), pp 2-21, and E Biham and A Shamir, "Differential Cryptanalysts of DES-like Cryptosystems," *Journal of Cryptology*, vol 4, No 1, 1991, pp 3-72

SOURCE OTA, 1994, and sources cited below

modules. [16] This approach makes the confidentiality function of the classified encryption algorithm available in a controlled fashion that does not increase users' abilities to employ cryptographic principles. A key-escrowing scheme is built in to ensure "lawfully authorized" electronic surveillance. [17] One of the reasons stated for specifying a classified, rather than published, encryption algorithm in the EES is to prevent its independent implementation without the law-enforcement access features.

Unlike the EES algorithm, the algorithm in the federal Digital Signature Standard has been published.[18] The public-key algorithm specified in the DSS uses a private key in signature generation, and a corresponding public key for signature verification. (See box 4-4.) However, the DSS technique was chosen so that public-key encryption functions would *not be* available to users. [19] This is significant because public-key encryption is extremely useful for key management.[20]

16 See *Federal Register*, vol. 59, Feb. 9, 1994, pp. 5997-6005 ("Approval of Federal Information Processing Standards Publication 185, Escrowed Encryption Standard (EES)").

17 Ibid., p. 6003.

18 See also appendix C.

19 According to F. Lynn McNulty, NIST Associate Director for Computer Security, the rationale for adopting the technique used in DSS was that, "We wanted a technology [hat did signatures-and nothing else—very well. " (Response to a question from Chairman Rick Boucher in testimony before the Subcommittee on Science of the House Committee on Science, Space, and Technology, Mar. 22, 1994. See also footnote 1 05.)

20 Public-key encryption can be used for confidentiality and for secure key exchange. See box 4-1.

## BOX 4-4: What Are Digital Signatures

Cryptography can be used to accomplish more than one safeguard objective **Encryption** techniques can be used to safeguard the confidentiality of the contents of a message (or a stored file), Message **authentication** techniques based on cryptography can be used to ensure the integrity of the message (that it has been received exactly as it was sent) and the authenticity of its origin (that it comes from the stated source) The oldest and simplest forms of message authentication use "secret" authentication parameters known only to the sender and intended recipient to generate "message authentication codes. " So long as the secret authentication parameter is kept secret from all other parties, these techniques protect the sender and the receiver from alteration or forgery of a message by all such third parties Because the same secret information is used by the sender to generate the message authentication code and by the receiver to validate it, these techniques cannot settle "disputes" between the sender and receiver as to what message, if any, was sent. For example, message authentication codes could not settle a dispute between a stockbroker and client in which the broker claims the client issued an order to purchase stock and the client claims he never did so

**Digital signatures** provide a higher degree of authentication by allowing resolution of disputes Although it is possible to generate digital signatures from a symmetric cipher like the federal Data Encryption Standard (DES), most interest centers on systems based on asymmetric ciphers, also known as *public-key cryptosysterns.* [2] These asymmetric ciphers use a pair of keys--one to encrypt, another to decrypt—in contrast to symmetric ciphers in which the same key is used for both operations. Each user has a unique pair of keys, one of which is kept private (secret) and the other is made public (e.g., by publishing in the electronic equivalent of a telephone book). The security of public-key systems rests on the authenticity of the public key and the secrecy of the private key, much as the security of symmetric ciphers rests on the secrecy of the single key (see discussion of key certification and management in chapter 2 and of digital signatures and nonrepudiation in chapter 3).

in principle, to sign a message using a public-key encryption system, a user could transform it with his private key, and send both the original message and the transformed version to the intended receiver The receiver would validate the message by acting on the transformed message with the sender's public key (obtained from the "electronic phone book") and seeing that the result exactly matched the original message. Because the signing operation depends on the sender's private key (known only to him or her), it is impossible for anyone else to sign messages in the sender's name But everyone can validate such signed messages, since the validation depends only on the sender's "public" key.

In practice, digital signatures sign shorter "message digests" rather than the whole messages, For digital signatures based on public-key systems, the sender first uses a cryptographic "hashing" algorithm to create a condensed "message digest" from the message [3] With the commercial RArest-Sharn/f-

---

[1] For details about the technology and applications for encryption, message authentication, and digital signatures, see D W Davies and W L Price, *Security for Computer Networks : An Introduction to Data Security in Teleprocessing and Electronic Funds Transfer,* 2nd Ed (New York, NY John Wiley & Sons, 1992) See also U S Congress, Office of Technology Assessment, *Defending Secrets, Sharing Data New Locks and Keys for Electronic Information, OTA-CIT-.31O* (Washington, DC U S Government Printing Office, October 1987), especially appendices C and D

*2* Merkle's "tree *Signature* techniques" made use of symmetric (secret-key) ciphers like the DES more usable for digital signatures However, there is currently more Interest in asymmetric cryptography for signatures (Martin Hellman, Professor of Electrical Engineering, Stanford University, personal communication, Apr 24, 1994, and Burton Kaliski, Jr, Chief Scientist, RSA Laboratories, personal communication, Apr 20,1994 )

[3] The RSA method is the best known public-key signature scheme, but others are possible, see T ElGamal, "A Public-Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms, *IEEE Transactions on /formation Theory,* vol *IT-31,* 1985, pp 469-472, and C P Schnorr, "Efficient Identification and Signatures for Smart Cards, " *Proceedings of Crypto 89, Advances in Cryptology* (New York, *NY* Springer-Verlag, 1990), pp 239-251

*(continued)*

## BOX 4-4 (cont'd.): What Are Digital Signatures?

Adleman (RSA) system, the signature is created by encrypting the message digest, using the sender's private key Because in the RSA system each key is the inverse of the other, the recipient can use the sender's public key to decrypt the signature, thereby recovering the original message digest The recipient compares this with the one he or she has calculated using the same hashing function—if they are identical, then the message has been received exactly as sent and, furthermore, the message did come from the supposed sender (otherwise his or her public key would not have yielded the correct message digest) [4]

The federal Digital Signature Standard (DSS) defines a somewhat different kind of public-key cryptographic standard for generating and verifying digital signatures [5] The DSS is to be used in conjunction with the federal "Secure Hash Standard" (FIPS Publication 180), which creates a short message digest, as described above. [6] The message digest is then used, in conjunction with the sender's private key and the algorithm specified in the DSS, to produce a message-specific signature Verifying the DSS signature involves a mathematical operation on the signature and message digest, using the sender's public key and the hash standard [7]

The DSS differs from the RSA digital signature method in that the DSS signature operation is not reversible, and hence can only be used for generating digital signatures. DSS signature verification is different than decryption. [8]

In contrast, the RSA system can encrypt, as well as do signatures Therefore, the RSA system can also be used to securely exchange cryptographic keys that are to be used for confidentiality (e g , "secret" keys for use with a symmetric encryption algorithm like the DES) This lack of encryption capability for secure key exchange was one reason why the government selected the DSS technique for the standard [9]

[4] See Davies and Price, op cit , ch 9 or app D of Office of Technology Assessment, op cit , footnote 1 The overall security of these schemes depends on maintaining secrecy of the private keys and on the authenticity of the public keys

[5] U S Department of Commerce, National Institute of Standards and Technology, "Digital Signature Standard (DSS)," FIPS Publication 186, May 19, 1994 The standard is effective Dec 1, 1994

[6] U S Department of Commerce, National Institute of Standards and Technology, "Secure Hash Standard," FIPS PUB 180, May 11, 1993 NIST recently announced a technical correction to the Secure Hash Standard According to NIST, NSA analysts discovered a "minor flaw" in the algorithm The algorithm was developed by NSA (NIST media advisory, Apr 22, 1994 ) According to NIST, the hash standard, "while still very strong, was not as robust as we had originally intended" and was being corrected (Raymond Kammer, Deputy Director, NIST, testimony before the Subcommittee on Technology and the Law, Committee on the Judiciary, U S Senate, May 3, 1994, p 11 )

[7] See National institute of Standards and Technology, *CSL Bulletin*, January 1993, or NIST, op cit , footnote 5

[8] Burton Kaliski, Jr, Chief Scientist RSA Laboratories, personal communication, May 4, 1994

[9] See chapte, 4, and *Federal Register*, vol 59, May 19, 1994, p 26209 ("The DSA does not provide for secret key distribution since it was not Intended for that purpose " Ibid )

SOURCE Off Ice of Technology Assessment, 1994, Martin Hellman (Stanford University), 1994; and references cited in notes

While other means of exchanging electronic keys are possible,[21] none is so mature as public-key technology. In contrast to the technique chosen for the DSS, the technique used in the most widely used commercial digital signature system (based on the Rivest-Shamir-Adleman, or *RSA*,

[21] See e.g., Tom Leighton, Department of Mathematics, Massachusetts Institute of Technology (MIT) and Silvio Micali, MIT Laboratory for Computer Science, "Secret-Key Agreement Without Public-Key Cryptography (Extended Abstract)," obtained from S. MicaIi, 1993.

algorithm) can also encrypt. Therefore, the RSA techniques can be used for secure key exchange (i.e., exchange of "secret" keys, such as those used with the DES), as well as for signatures. Another public-key technique, devised by Whitfield Diffie and Martin Hellman, can also be used for key exchange.[22] The Diffie-Hellman technique does not encrypt.

In OTA's view, both the EES and the DSS are federal standards that are part of a long-term control strategy intended to retard the general availability of '*unbreakable" or "hard to break" cryptography within the United States, for reasons of national security and law enforcement. As stated by NIST Deputy Director Raymond Kammer:

> Government standards should not harm law enforcement/national security.
>
> This is fairly straightforward, but can be difficult to achieve. In setting standards, the interests of all the components of the government should be taken into account. In the case of encryption, this means not only the user community, but also the law enforcement and national security communities, particularly since standards setting activities can have long-term impacts (which, unfortunately, can sometimes be hard to forecast) .23

It appears that the EES is intended to complement the DSS in this overall encryption-control strategy, by discouraging future development and use of encryption without built-in law enforcement access, in favor of key-escrowed and related encryption technologies. If the EES and/or other key-escrow encryption standards (e.g., for use in computer networks) become widely used, this could ultimately reduce the variety of alternative cryptography products through market dominance that makes alternatives more scarce or more costly. In May 1994 testimony before the Senate Subcommittee on Technology and the Law, Whitfield Diffie (Sun Microsystems, Inc.) referred to the EES and related key-escrow initiatives, as well as the DSS and the digital telephony proposals, as:

> . . . a unified whole whose objective is to maintain and expand electronic interception for both law enforcement and national security purposes.[24]

In testimony in support of the EES and related technology before the House Subcommittee on Technology, Environment, and Aviation, Dorothy Denning (Georgetown University) stated that:

> As we move into an era of even greater electronic communications, we can and must design our telecommunications infrastructure and encryption systems to support our needs as a nation for secure communications, individual privacy, economic strength, effective law enforcement, and national security. The Clipper Chip is an important step towards meeting all our national needs, and the government should continue to move forward with the program.
>
> The government needs an encryption standard to succeed DES. If in lieu of Clipper, the government were to adopt and promote a standard that provides strong encryption without government access, society could suffer severe economic and human losses resulting from a diminished capability of law enforcement to investigate and prosecute organized crime and terrorism, and from a diminished capability for foreign intelligence. . . . [T]he government rightly concluded that it would be irresponsible to promote a standard that foils law enforcement when technology is at hand to accommodate law enforcement needs without jeopardizing security and privacy. Moreover, through the Adminis-

---

22 The public-key concept was first published by Whitfield Diffie and Martin Hellman in "New Directions in Cryptography," Theory, vol. IT-22, No. 6, *IEEE Transactions on Information*, November 1976, pp. 644-654. Diffie and Hellman described how such a system could be used for key distribution and to "sign" individual messages.

23 Kammer testimony, May 3, 1994, op. cit., footnote 13, pp. IO-11.

24 Whitfield Diffie, Distinguished Engineer, Sun Microsystems, Inc., testimony before the Subcommittee on Technology and the Law, Committee on the Judiciary, U.S. Senate, May 3, 1994, p. 2. (Diffie was also referring to the Capstone and TESSERA implementations of the EES encryption algorithm.)

tration's commitment to Clipper or some other form of key escrow, escrowed encryption may dominate in the market, mitigating the effect of unescrowed encryption on law enforcement.[25]

Concerns over the proliferation of encryption that have shaped and/or retarded federal standards development have complicated federal agencies' technological choices. For example, as appendix C explains, national-security concerns regarding the increasingly widespread availability of robust encryption-and, more recently, patent problems-contributed to the extraordinarily lengthy development of a federal standard for digital signatures: NIST first published a solicitation for public-key cryptographic algorithms in 1982, and the DSS was finalized in FIPS Publication 186 in May 1994.[26] (At this writing, the question of whether the DSS would be the subject of patent litigation was still open-see appendix C).

Public-key cryptography can be used for digital signatures, for encryption. and for secure key distribution/exchange. The DSS is intended to supplant, at least in part, the demand for other public-key cryptography by providing a method for generating and verifying digital signatures. However, while the DSS algorithm is a public-key signature algorithm, it is not a public-key encryption algorithm.[27] That means, for example, that it cannot be used to securely distribute "secret" encryption keys for use with symmetric encryption like the DES or EES algorithms. Some sort of interoperable (i.e., standardized) method for secure key exchange is still needed.[28]

As of June 1994, the DSS had been finalized, but there was no FIPS for public-key key exchange. Two implementations of the EES encryption algorithm that are used for data communications in computer networks-the *Capstone chip* and the *TESSERA* card-contain a public-key Key Exchange Algorithm (KEA).[29] However, as of June 1994, this KEA is not part of any FIPS .[30] Therefore, organizations that do not use Capstone or TESSERA still need to select a secure and interoperable form of key distribution.

The lengthy evolution of the DSS meant that federal agencies had begun to look to commercial products (e.g., based on the RSA system) to meet immediate needs for digital signature technology.[31] The introduction of the EES additionally complicates agencies' technological choices, in that the EES and related government key-escrow encryption techniques (e. g.. for data communications in computer networks, or for file encryption) may not become popular in the private sector for some time, if at all. As of this writing, the EES has

[25] Dorothy E. Denning, Professor and Chair, Department of Computer Science, Georgetown University, testimony before the Subcommittee on Technology, Environment, and Aviation, Committee on Science, Space and Technology, U.S. House of Representatives, May 3, 1994, pp. 6-7. Denning was one of the five nongovernmental experts who evaluated the EES algorithm under security clearance. (See discussion later in chapter.)

[26] See "Approval of Federal Information Processing Standards Publication 186, Digital Signature Standard (DSS)," *Federal Register*, vol. 59, May 19, 1994, pp. 26208-1 I, and NIST, "Digital Signature Standard (DSS)," FIPS PUB 186 (Gaithersburg, MD U.S. Department of Commerce, May 1 9, 1994).

[27] See box 4-4.

[28] One public-key algorithm that can be used for key distribution is the RSA algorithm; the RSA algorithm can encrypt. The RSA system was proposed in 1978 by Rivest, Shamir, and Adleman. The Diffie-Hellman algorithm is another method; this can be used for key generation and exchange and does not encrypt. See also ch. 2.

[29] The Capstone chip is an implementation of the Escrowed Encryption Standard algorithm. It is used for data communications and contains the EES algorithm (called *SKIPJACK),* as well as digital-signature and hey-exchange functions. (The Clipper chip is used in telephone systems and has just the EES algorithm. ) TESSERA is a PCMCIA card that contains a Capstone chip. It includes additional features and is being used in the Defense Message System. (Clinton Brooks, Special Assistant to the Director, NSA, personal communication, May 25, 1994. )

[30] Miles Smid Manager Security Technology Group, NIST, personal communication, May 20, 1994

[31] For example, at this writing, the IRS was considering using both the DSS and RSA signature techniques. (Tim Minahan, "IRS Digital Signature Scheme Calls for Both DSS and RSA Verification," *Government Computer News*, July 18, 1994, pp. 1, 65. )

not yet been embraced within government and is largely unpopular outside of government.[32] Therefore, agencies may need to support multiple encryption technologies both for transactions (i.e., signatures) and for communications (i.e., encryption, key exchange) with each other, with the public, and with private-sector organizations.

## GOVERNMENT CONCERNS AND INFORMATION SAFEGUARDS

As the previous section indicated, the federal government faces a fundamental tension between the desire to foster the development and deployment of effective (and cost-effective) technologies for use in safeguarding unclassified information, so that these can be widely used by civilian agencies and the private sector, and the desire to control the proliferation of technologies that can adversely affect government's signals-intelligence and law-enforcement capabilities. This tension runs throughout the government's own activities as a developer, user, and regulator of safeguard technologies. Although the relative balance between national-security and other objectives (e.g., open government, market competitiveness, privacy) has shifted from time to time, national-security objectives have always been preeminent in establishing federal policies regarding information security (or computer and communications security).

In a networked society, where communications, information, and commerce are digital, the struggle to control cryptography is at the heart of this tension. Control of cryptography encompasses: 1) control of research in cryptography and especially in cryptanalysts (code-breaking), 2) control of publication in cryptography and related fields, 3) control of patenting of cryptographic inventions (new techniques for encryption and/or new ways of implementing these in useful products), and 4) export controls on the proliferation of cryptography-based products and expertise.[33]

Over the past three decades, this struggle for control has been exacerbated by:

1. *technological advances in computing and microelectronics* that have made inexpensive, software-based, PC-based, smart-card-based,

---

32 See, e.g., Beau Brendler, "This Ship's Going Nowhere: Why Clinton's Clipper Policy Makes No Sense," *Washington Technology*, Feb. 10, 1994, pp. 1,6; John Markoff, "Cyberspace Under Lock and Key," *The New York Times*, Feb. 13, 1994, p. E3; Philip Elmer-Dewitt, "Who Should Keeptbe Keys," *Time Magazine*, Mar. 14, 1994, pp. 90-91; and John Markoff, "An Administration Reversal on Wiretapping Technology," *The New York Times*, July 21, 1994, pp. D1,D7.

The Committee on Communications and Information Policy of the IEEE United States Activities Board has taken the position that current cryptographic policies reflect the dominance of law-enforcement and national-security concerns and do not adequately reflect the needs of electronics manufacturers, service providers, or network users. The committee advocates development of public, exportable, secure algorithms and the implementation of such algorithms as national standards. (Bob Carlson, "U.S. Government Reaffirms Stand on Clipper Chip Proposal," *IEEE Computer*, April 1994, p. 63.)

33 The cryptographic-research community has grown over the last decade, but it is still relatively small compared with other fields in computer science, electrical engineering, and mathematics. In the 1970s and 1980s, there were serious controversies concerning attempts by NSA to control federal research funding in cryptography and to control publication and patenting by researchers in academia and industry. For historical development of cryptography and the repeated controversies concerning government attempts (through NSA) to control cryptography through research funding, prepublication review, and patent secrecy orders, see Susan Landau, "Zero Knowledge and the Department of Defense," *Notices of the American Mathematics/ Society, vol. 35, No. 1*, January 1988, pp. 5- 12; U.S. Congress, House of Representatives, Committee on Government Operations, *Computer Security Act of 1987—Report to Accompany H.R.145*, H. Rept. No. 100-153, Part 11, 10Oth Cong., 1st sess., June 11, 1987 (Washington, DC: U.S. Government Printing Office, 1987), pp. 19-25; James Bamford, *The Puzzle Palace (New* York, NY: Penguin Books, 1983); Tom Ferguson, "Private Locks, Public Keys and State Secrets: New Problems in Guarding Information with Cryptography," Harvard University Center for Information Policy Research, Program on Information Resources Policy, April 1982; Public Cryptography Study Group, American Council on Education, "Report of the Public Cryptography Study Group" and "The Case Against Restraints on Nongovernmental Research in Cryptography: A Minority Report by Prof. George I. Davida," *Academe, vol.* 67, December 1981, pp. 372-.382; U.S. Congress, House of Representatives, Committee on Government Operations, *The Government's Classification of Private Ideas*, H. Rept. No. 96-1540, 96th Congress, 2d sess. (Washington, DC: U.S. Government Printing Office, Dec. 22, 1980); and David Kahn, *The Codebreakers: The Story of Secret Writing (New* York, NY: MacMillan, 1%7). See also OTA, op. cit., footnote 1, especially pp. *55-59* and 168-172.

and token-based (e.g., using PCMCIA cards) cryptography potentially ubiquitous; and
2. *increasing private-sector capabilities in cryptography*, as evidenced by independent development of commercial, public-key encryption systems.

These have made possible the:

3. *increasing reliance on digital communications and information processing* for commercial transactions and operations in the public and private sectors.

Together, these developments have enabled and supported a growing industry segment offering a variety of hardware- and software-based information safeguards based on cryptography. Recent encryption initiatives like the EES and DSS seem orchestrated to increase control by reducing commercial variety and availability over the long run, so as to retard the development and spread of other encryption technologies that could impair signals intelligence and law enforcement.

A historical review of the policy issues, debates, and developments during the 1970s and 1980s that led to the current environment is beyond the scope of this report, which focuses on their current manifestations in private and public-sector activities.[34] This chapter examines these in light of the ongoing debates over the activities of NIST and NSA, particularly regarding export controls and standards development. These are important because the government uses them to control cryptography.

Federal standards (i.e., the FIPS) influence the technologies used by federal agencies and provide a basis for interoperability, thus creating a large and stable, "target market" for safeguard vendors. If the attributes of the standard technology are also applicable to the private sector and the standard has wide appeal, an even larger but still relatively stable market should result. The technological stability means that firms compete less in terms of the attributes of the fundamental technology and more in terms of cost, ease of use, and so forth. Therefore, firms need to invest less in research and development (especially risky for a complex technology like cryptography) and in convincing potential customers of product quality. (See discussion of standards and certification in chapter 2). This can result in higher profits for producers, even in the long run, and in increased availability and use of safeguards based on the standard.

Promulgation of the DES as a stable and certified technology—at a time when the commercial market for cryptography-based safeguards for unclassified information was emerging—stimulated supply and demand. Although the choice of the algorithm was originally controversial due to concerns over NSA's involvement, the DES gained wide acceptance and has been the basis for several industry standards, in large part because it was a public[35] standard that could be freely evaluated and implemented. Although DES products are subject to U.S. export controls, DES technology is also widely available around the world and the algorithm has been adopted in several international standards. The process by which the DES was de-

[34] For a short review of the historical tension between national security and other national objectives and the struggle to control cryptography, see OTA, op. cit., footnote 1. For a longer review of the developments of federal computer security and communication security policies and programs after World War 11, including discussion of challenges to the government's cryptographic monopoly over the last two decades, see George F, Jelen, "Information Security: An Elusive Goal," Harvard University Center for Information Policy Research, Program on Information Resources Policy, June 1985. Jelen also examines the power struggle between NSA and the Commerce Department's National Telecommunications and Information Administration during the late 1970s and early 1980s and the motivations for and effects of national-security directives in the 1980s that gave the Department of Defense the leadership role in communication security (COMSEC) and computer security (COMPUSEC).

[35] *Public* in this sense refers to the fact that the DES algorithm was published.

veloped and evaluated also stimulated private-sector interest in cryptographic research, ultimately increasing the variety of commercial safeguard technologies.

By 1993, 40 manufacturers were producing about 50 implementations of the DES in hardware or firmware that had been validated for federal use (as meeting the FIPS) by NIST. Another 60 companies were estimated to be producing software implementations of the DES. A 1993 industry estimate of U.S. sales of DES hardware and software products was between $75 million and $125 million annually.[36] As of April 1994, a survey of products using cryptography in the United States and abroad, conducted by the Software Publishers Association (SPA) had identified 245 domestic encryption products (hardware and software) that used the DES.[37]

Now, however, introduction of an incompatible *new* federal standard-e. g., the EES—may be destabilizing. If the EES and related technologies ultimately manage to gain wide appeal, they may succeed in "crowding out" safeguards based upon other cryptographic techniques.[38] This may be a long-term objective of the key-escrow encryption initiative, in order to stem the supply of alternative cryptography products by ensuring vendors a large and lucrative federal market and by encouraging private-sector demand to eventually switch to key-escrowing technology.[39] In the long term, a loss of technological variety is significant to private-sector cryptography, because more diverse research and development efforts tend to increase the overall pace of technological advance. In the near term, technological uncertainty may delay widespread investments in *any* new safeguard, as users wait to see which technology prevails.[40]

In May 1994 testimony before the Subcommittee on Technology and the Law of the Senate Judiciary Committee, Assistant Attorney General Jo Ann Harris stated that:

> The Clinton Administration has been farsighted in seeing the advent of high-quality, user-friendly encryption products and the implications of such products. It has also been prepared to act early, when markets are still developing and when both consumers and manufacturers are seeking strong, reliable cryptography for use in mass-market products.
>
> We believe, therefore, Mr. Chairman [Patrick J. Leahy], that, as one major equipment manufacturer has already done, others will respond to their customers' needs for extremely strong encryption by marketing key escrow-

---

J61ndu~~ estimates cited in: Charlotte Adams, "Data Encryption Standard Software Now Headed for Widespread Government Use," *Federa/ Computer Week,* July 26, 1993, p. 35. The reaffirmation of the DES in FIPS Publication 46-2 (NIST, op. cit., footnote 14) makes software implementations of the DES also eligible for validation.

37 Stephen T. Walker, President, Trusted Information Systems, Inc., testimony presented before the Subcommittee on Technology and the Law, Committee on the Judiciary, U.S. Senate, May 3, 1994, p. 15 and enclosure. See also Lance Hoffman, "SPA Study of Foreign Availability of Cryptography," *SPA News,* March 1994. SPA began its study of foreign availability in 1993.

*38* At present, the EES is not being well received by the private sector, in part because there is a growing installed base of other technologies (e.g., the DES and the RSA system) and in part because of the classified algorithm and key escrowing. In establishing the EES, the government is acting in its roles as a producer and regulator of safeguard technologies. This contrasts with the government's role (with industry) as a user in other, voluntary standards development. (See, e.g., John Perry Barlow, "A Plain Text on Crypto Policy," *Communications of the ACM, vol. 36, No. 11,* November 1993, pp. *21-26;* and Lance J, Hoffman, "Clipping Clipper," Communications *of the* ACM, vol. 36, No. 9, September 1993, pp. *15-17.) The* role of the U.S. government in developing the algorithm, as well as the key escrowing provisions, also make the EES unattractive to the international business community. (Nanette DiTosto, United States Council for International Business, personal communication, Apr. 28, 1994.)

39 In early 1994, the Department of Justice had reportedly purchased 8,000 EES devices and was considering purchasing another 2,000, in a procurement totaling *$8* million. (Executive-branch procurements announced by Raymond Kammer, NIST Deputy Director, as quoted in: Brad Bass, "Clipper Gets Stamp of Approval," *Federal Computer Week,* Feb. 7, 1994, pp. 1,4.)

40 This happened with videocassette recorders (VCRS). When technological uncertainty decreased (after the rivalry between VHS and Betamax was resolved), VCR penetration began to increase dramatically,

> equipped products. And as that occurs, we look for a gravitation of the market to key-escrow encryption, based on both a need for interoperability and a recognition of its inherent quality. Even many of those who may desire encryption to mask illicit activities will choose key-escrow encryption because of its availability, its ease of use, and its interoperability with equipment used by legitimate enterprises. [41]

However, others question the need to act now:

> If allowing or even encouraging wide dissemination of high-grade cryptography proves to be a mistake, it will be a correctable mistake. Generations of electronic equipment follow one another very quickly. If cryptography comes to present such a problem that there is popular consensus for regulating it, this will be just as possible in a decade as it is today. If on the other hand, we set the precedent of building government surveillance capabilities into our security equipment we risk entrenching a bureaucracy that will not easily surrender the power this gives.[42]

At this writing, the success of this strategy to control cryptography is still questionable—in the near term, at least. One reason the outcome will take some time to materialize is that although it was issued as a FIPS, use of the EES is *voluntary* (even within the government) and many federal agencies have not yet taken positions regarding its implementation, or announced plans to implement the EES in their operations.[43] For example, the Federal Reserve System encrypts its funds transfer operation, using DES-based technology, and is an active participant in the American National Standards Institute (ANSI) banking standards process. Although the Federal Reserve monitors advances in security technologies, as of spring 1994 it remained committed to "cryptographic implementations which are based on DES and are ANSI compliant."[44]

In July 1994, Vice President Gore indicated the Clinton Administration's willingness to explore industry alternatives for key-escrow encryption, including techniques based on unclassified algorithms or implemented in software. These alternatives would be used to safeguard information in computer networks and video networks; the EES and Clipper chip would be retained for telephony. Whether the fruits of this exploration result in increased acceptance of key-escrow encryption will not be evident for some time.

Moreover, not all government attempts at influencing the marketplace through procurement policies (and the FIPS) are successful. The FIPS that prove to be unpopular with industry and users can have little influence on the private sector.[45] For example, the government made an early commitment to the Open Systems Interconnection (OSI) protocols for networking, but it is the ubiquitous Transmission Control Protocol/Internet Protocol (TCP/IP) protocols that have enjoyed wide use throughout the world in the Internet and other networks. Although the Government Open Systems Interconnection Profile (GOSIP) was mandated for agencies, it did not become popular in the commercial market, so there was a lack of GOSIP products, relative to TCP/IP products. As a result, the government had to reassess open systems network requirements and federal use of networking standards, through the Federal Inter-

---

41 Jo Ann Harris testimony, op. cit., footnote 8, pp. 3-4.

42 Diffie testimony, op. cit., footnote 24, p. 10.

43 Successful adopters of other technology (e.g., the DES) may resist switching to the new technology, not wanting to "waste" or duplicate earlier investments. Also, some federal standards choices have been regarded as "picking failures," such as the choice of OSI rather than TCP/IP. Thus, adopters are wary of investing heavily in federal standards that ultimately may not even be widely used within government.

44 Letter from John Pelick (Chairman, Federal Reserve System Security Steering Group) to M. Garrett (Federal Reserve Bank of Minneapolis), Feb. 17, 1994; and Marianne Emerson (Assistant Director, Division of Information Resources Management, Board of Governors of the Federal Reserve System), personal communications, Apr. 17, 1994 and June 23, 1994.

45 See Carl F. Cargill, *Information Technology Standardization: Theory, process, and Organizations* (Bedford, MA: Digital Press, 1989).

networking Requirements Panel. For the future, agencies will be able to adopt both sets of protocols according to the relative advantages and disadvantages of each.[46]

Some of the resistance to the DSS and EES can be understood in terms of users' unwillingness to invest in multiple technologies and/or to make obsolete prior investments in other technologies, such as the RSA and DES algorithms. Additionally, the evolution of cryptographic standards may be different from other information-technology standards, in that the private sector historically has been less capable than NSA in developing and evaluating the security of cryptographic technologies.

Other government policies can also raise costs, delay adoption, or reduce variety. In the case of cryptography-based safeguards, export controls segment domestic and export markets. This creates additional disincentives to invest in the development-or use--of robust but nonexportable safeguards (see discussion below). As Stephen Walker (Trusted Information Systems, Inc.) testified in May 1994:

> When U.S. industry foregoes the opportunity to produce products that integrate good security practices, such as cryptography, into their products because they cannot export those products to their overseas markets, U.S. users (individuals, companies, and government agencies) are denied access to the basic tools they need to protect their own sensitive information.
>
> The U.S. government does not have the authority to regulate the use of cryptography within this country. But if through strict control of exports they can deter industry from building products that effectively employ cryptography, then they have achieved a very effective form of internal use control.[47]

The remainder of this chapter examines:

- *The policy framework within which federal agencies formulate and implement their information-security and privacy policies and guidelines.* This establishes computer-security and information-security standards-setting authority through the Brooks Act of 1965 and the Computer Security Act of 1987. Special attention is given to the history and implementation of the Computer Security Act, because these are fundamental to understanding current issues related to federal cryptographic standards used to safeguard unclassified information.
- *The export control regime that seeks to control proliferation of cryptography.* This regime affects the competitiveness of U.S. companies that seek to create or incorporate safeguards based on cryptography and, therefore, affects the supply and use of these safeguards.
- *The ongoing information-security research and federal standards activities of NIST and NSA. The* Computer Security Act of 1987 was designed to balance national security and other national objectives, giving NIST the lead in setting security standards and guidelines for unclassified information and defining NSA's role as technical advisor to NIST. However, events subsequent to the act have not convincingly demonstrated NIST's leadership in this area.[48]

## GUIDANCE ON SAFEGUARDING INFORMATION IN FEDERAL AGENCIES

Statutory guidance on safeguarding information provides a policy framework—in terms of technical and institutional requirements and managerial responsibilities—for government information and information-system security.

---

46 Arielle Emmett, "Applications Drive Federal TCP/IP Use," *Federal Computer Week*, May 9, 1994, pp. 22-23.

47 Walker testimony, op. cit., footnote 37, p. 26.

48 See also U.S. General Accounting Office, *Communications Privacy: Federal Policy and Actions*, GAO/OSI-94-2 (Washington, DC: U.S. Government Printing Office, November 1993).

Overlaid on this are statutory privacy requirements that set forth policies concerning the dissemination and use of certain types of information about individuals. Within this framework, and subject to their own specific statutory requirements, federal agencies and departments develop their policies and guidelines, in order to meet individual and government-wide security and privacy objectives (see box 4-5).

Information security in the broadest sense is fundamental to privacy protection, because conscientious use of appropriate technical and institutional information safeguards can help achieve privacy goals. The Privacy Act of 1974 set forth data collection, confidentiality, procedural, and accountability requirements federal agencies must meet to prevent unlawful invasions of personal privacy, and provides remedies for noncompliance. It does not mandate use of specific technological measures to accomplish these requirements. Other statutes set forth information confidentiality y and integrity requirements for specific agencies, such as the Internal Revenue Service, Bureau of the Census, and so forth. (Issues related to the Privacy Act, and other, international privacy issues are discussed in chapter 3.)

This section spotlights three key developments in the evolution of the overall statutory and regulatory framework within which federal agencies formulate their information-security and privacy policies and guidelines, and then select and deploy safeguard technologies to implement them:

1. **The Brooks Act of 1965** made the Commerce Department the focal point for promulgation of government "automatic data processing" (i.e., computer and information-system) standards and authorized Commerce to conduct a research program to support standards development and assist federal agencies in implementing these standards. These responsibilities were carried out by the National Bureau of Standards (NBS, now NIST).
2. **The Paperwork Reduction Act of 1980** assigned the Office of Management and Budget (OMB) responsibilities for maintaining a comprehensive set of information resources management policies and for promoting the use of information technology to improve the use and dissemination of information by federal agencies. OMB **Circular A-130** ***(Management*** *of Federal Information Resources)* was originally issued in 1985 to fulfill these and other statutory requirements (including the Privacy Act).
3. **The Computer Security Act of 1987** affirmed and expanded the computer-security research and standards responsibilities of NBS and gave it the responsibility for developing computer system security training programs and for commenting on agency computer system security plans. The U.S. General Accounting Office (GAO) has audited agencies' progress in implementing the security controls mandated by the Computer Security Act of 1987.[49]

Special emphasis is given to the Computer Security Act in this chapter, because it is fundamental to the development of federal standards for safeguarding unclassified information, to the balance between national-security and other objectives in implementing security and privacy policies within the federal government, and to issues concerning government control of cryptography. Moreover, review of the controversies and debate surrounding the Computer Security Act—and

49 See *the* following GAO reports: *Computer Security: Governmentwide Planning Process Had Limited Impact,* GAO/IMTEC-90-48 (Washington, DC: U.S. Government Printing Office, May 10, 1990); *Computer Security: Compliance with Security P/an Requirements of the Computer Security Act,* GAO/IMTEC-89-55, June 21, 1989; *Compliance with Training Requirements of the Computer Security Act of 1987,* GAO/IMTEC-89-16BR, Feb. 22, 1989); and *Computer Security: Status of Compliance with the Computer Security Act of* /987, GAO/IMTEC-88-61BR, Sept. 22, 1988.

### BOX 4-5: What Are Federal-Agency Concerns?

As part of this study, the Office of Technology Assessment held workshops on federal-agency issues related to information security and privacy in network environments. Participants came from a variety of agencies and had a variety of responsibilities and interests with respect to information privacy and security. Their concerns, comments, and topics of interest included the following

**Network Environments Require Changes**

- The decentralized nature of Internet development has advantages and disadvantages, We aren't fixing on a technology too soon, and it's flexible, but having "no one in charge" means that responsibility for safeguards is decentralized, too Unfortunately, sometimes responsibility is more decentralized than authority, and agency managers don't have the authority they need to ensure good technology and practices.
- Going from the Internet to the prospect of truly global networks, how could we ever have centralized control? How do we develop appropriate safeguards, legal sanctions, penalties when information flows across borders, jurisdictions?
- At the agency level, the move away from mainframes into the distributed environment distributes responsibility for security and privacy to all users. This can be a problem without attention to policies, procedures, and training
- There is a distinction between appropriate security for the network itself ("essential services" to ensure continuityof service, protection of passwords, etc. ) and appropriate user choices of security "at the ends" for applications, data storage, etc. The latter are the responsibility of the "reasonable user" who must decide what security investments to make based on cost, value of information resources, etc. Nevertheless, it often hard to cost-justify security, especially in times of tight budgets and/or no direct experience with security problems.
- Safeguard choices must be based on standards of due diligence and due care for information providers, custodians, users Maintaining accountability and determining responsibilities of secondary users in distributed environments are crucial—we have to deal with a continuum of ownership, confidentiality requirements, etc.
- Federal standards development often lags agency needs, so agencies wind up having to support several technologies in order to operate and communicate with the private sector and each other. What is needed is proactive, rather than reactive, standards and guidance
- Export controls on cryptographic products cause complications for federal agencies that need to network with industry partners in cooperative research and development agreements when these partners are global organizations, or need to communicate with private-sector organizations, vendors, suppliers, etc. Cryptographic safeguards can also introduce other complications in networking-they are designed to prevent "workarounds, " so interoperability problems are harder to fix,
- The lack of a government-wide security classification scheme will make it harder to determine appropriate levels of security when Information is shared and used on an interagency basis,

(continued)

subsequent controversies over its implementation—provide background for understanding the current issues concerning Federal Information Processing Standards, such as the EES and DSS.

## The Brooks Act

The Brooks Act of 1965 (Public Law 89-306) was enacted to *'provide for the economic and efficient

## BOX 4-5 (cont'd): What Are Federal-Agency Concerns?

**Users Make Safeguards Work-or Not Work**

- We need to make training and awareness continuing and more effective-how can we better motivate users to understand and comply with privacy and security requirements?
- Do we need to make security "transparent and easy" for users in order to encourage compliance? Are rewards better incentives than punishments?
- In decentralized environments, can fostering personal ethics and responsibility as bases for effective security and proper treatment of personal Information be more effective than relying on sanctions or waiting for technology to "do it all"?

**Multiple Objectives Must Be Balanced**

- Measures to ensure confidentiality and control access (including copyright mechanisms) must be balanced with the right of the public to have unfettered access to certain types of Information
- We have to develop an equitable way of compensating copyrightholders while preserving what we have now in terms of fair use, acceptable library practices, etc. What is the business process that develops public access with fair compensation and preservation of fair use, particularly when products are being licensed, not sold?
- We need way to develop a "public voice" in privacy and security policy development Who is being included in the policy debate, and how can we build advocates for the citizen into the process?
- With respect to privacy--should there be a right to see files about yourself held in the private sector or by government? to correct them (e g , Fair Credit Reporting Act)? Going to the courts is costly—are administrative sanctions more equitable for the '(little guy"?

SOURCE Off Ice of Technology Assessment workshops, October and December 1994

purchase, lease, maintenance, operation, and utilization of automatic data processing [ADP] equipment by federal departments and agencies." The Brooks Act gives the General Services Administration (GSA) central purchasing and oversight authority over federal ADP and telecommunications equipment. The GSA Administrator may delegate purchasing authority to individual agencies for reasons of economy or operational efficiency, or when delegation is essential to national defense or national security.[50] Delegations of procurement authority for agency information systems and/or large purchases of particular computers have become increasingly common over the years, and GSA schedules have been established for commodity purchases of microcomputers, peripherals, packaged software and the like. GSA, however, always retains central authority under the act and does centralized procurements, as in establishing the Federal Telephone System contract. Section 11 l(c) of the act requires agencies to report annually to Congress and to the Office of Management and Budget (formerly the Bureau of the Budget) on ADP equipment inventories, acquisitions, and utilization, as well as ADP expenditures.

A provision of the Brooks Act that is fundamental to unclassified information-system security is the authorization of the Secretary of Commerce:

1. to provide GSA and other agencies with scientific and technological advisory services relating to automatic data processing and related systems, and

50 The Warner Amendment (Public Law 97-86) exempted certain types of Department of Defense procurements from the Brooks Act.

2. to make appropriate recommendations to the President relating to the establishment of uniform federal automated data processing standards.[51]

This section also authorizes the Secretary of Commerce to "undertake the necessary research in the sciences and technologies of automatic data processing and related systems, as maybe required under the provisions of this subsection."

Thus, the Brooks Act established the computer-systems research programs and standards development conducted by the National Bureau of Standards, now the National Institute of Standards and Technology. NBS established its program in computer and communications security in 1973, under authority of the Brooks Act; the agency was already developing performance standards for government computers. This security program led to the adoption of the Data Encryption Standard as a Federal Information Processing Standard for use in safeguarding unclassified information.[52]

The security responsibilities of what is now NIST's Computer Systems Laboratory (CSL) were affirmed and extended by the Computer Security Act of 1987. CSL has been responsible for developing standards, providing technical assistance, and conducting research for computers and related systems; it also provides technical support to civil agencies and industry. CSL and its predecessors have published dozens of FIPS and guidelines[53] on information-systems operations and security, most recently the controversial Escrowed Encryption Standard (FIPS Publication 185, 1994) and Digital Signature Standard (FIPS Publication 186, 1994).

Under authority of the Brooks Act as amended, NIST participates in the activities of voluntary standards organizations such as the American National Standards Institute and the International Organization for Standardization. For a more detailed history of the National Institute for Standards and Technology's computer security program and the evolution of the DES, including the role of the National Security Agency, see the OTA's 1987 report, *Defending Secrets, Sharing Data: New Locks and Keys for Electronic Information.*[54] The Computer Security Act of 1987 and NIST's responsibilities under the act are discussed later in this chapter.

The NIST director has indicated an intention of creating a new Information Technology Laboratory, based on the current Computer Systems Laboratory and the NIST Computing and Applied Mathematics Laboratory. The rationale for this would be to improve NIST's capabilities in the underlying technologies and enable NIST to be more responsive to the needs of industry and government with respect to the information infrastructure.[55]

---

51 Public Law 89-306, sec. 111 (f).

52 Following some debate concerning its robustness against attack, given current technologies, the DES was recently recertified (until 1998) in hardware and—for the first time—in software implementations. The DES uses a symmetric encryption algorithm. It has been the basis of numerous other federal, national, and international standards and is in wide use to ensure information confidentiality via encryption (e.g., N] ST, op. cit., footnote 14) and integrity via message authentication (e.g., N] ST, "Computer Data Authentication, " FIPS PUB 113 (Gaithersburg, MD: U.S. Department of Commerce, May 30, 1985)).

53 In addition t. the DES, these standards include, for example NIST, "Guidelines for Automatic Data Processing Physical Security and Risk Management," FIPS PUB31, June 1974; "Guideline for Automatic Data Processing Risk Analysis," FIPS PUB 65, Aug. 1, 1979; "Guidelines for Security of Computer Applications," FIPS PUB 73, June 30, 1980; "DES Modes of Operation," FIPS PUB81, Dec. 2, 1980; "Computer Data Authentication," op. cit., footnote 52; "Key Management Using ANSI X9. 17," op. cit., footnote 15; "Secure Hash Standard," FIPS PUB 180, May 11, 1993; "Automated Password Generator," FJPS PUB 181, Oct. 5, 1993; and "Security Requirements for Cryptographic Modules," FIPS PUB 140-1. Jan. 11, 1994. All the FIPS publications are published by the Department of Commerce, Gaithersburg, MD.

54 OTA op cit footnote 1. Chapter 4 and appendix C of the 1987 report describe the DES; appendix D discusses use Of the DES algorithm and others for message authentication and digital signatures. (Note: As of 1994, software implementations of the DES comply with the federal standard. )

55 Arati Prabhakar, Director, N] ST, personal communication, May 12, 1994; NIST public affairs division, June 6, 1994.

## The Paperwork Reduction Act and OMB Circular A-130

The Paperwork Reduction Act of 1980 (Public Law 96-511) gave agencies a broad mandate to perform their information-management activities in an efficient, effective, and economical manner. The Office of Management and Budget was given authority for:

1. developing and implementing uniform and consistent information resource management policies;
2. overseeing the development of and promoting the use of government information management principles, standards, and guidelines;
3. evaluating the adequacy and efficiency of agency information management practices; and
4. determining whether these practices comply with the policies, principles, standards, and guidelines promulgated by the director of OMB.

The original OMB Circular A- 130, *The Management of Federal Information Resources*,[56] was issued in 1985 to fulfill these and other statutory responsibilities, including requirements of the Privacy Act (see chapter 3). It revised and consolidated policies and procedures from several other OMB directives, which were rescinded. Appendix 111 of the circular addressed the "Security of Federal Automated Information Systems," Its purpose was to establish a minimal set of controls to be included in federal information systems security programs, assign responsibilities for the security of agency information systems, and clarify the relationship between these agency controls and security programs and the requirements of OMB Circular A-123 *(internal Control Systems).*[57] *The* appendix also incorporated responsibilities from applicable national security directives. Federal agencies can obtain services from GSA on a reimbursable basis, in support of the risk analysis and security audit requirements of Circular A- 130; GSA also provides a number of information-system security documents.

The security appendix of OMB Circular A-130 assigned the Commerce Department responsibility for developing and issuing standards and guidelines for the security of federal information systems, for establishing standards "approved in accordance with applicable national security directives," for systems used to process information that was national -security *sensitive* (but not classified), and for providing technical support to agencies in implementing these standards and guidelines. The Defense Department was to act as the executive agent of the government for the security of telecommunications and information systems that process information, "the loss of which could adversely affect the national security interest" (i.e., including information that was unclassified but was considered "sensitive"), and was to provide technical material and ass i stance to federal agencies concerning the security of telecommunications and information systems. These responsibilities later shifted (see below) in accordance with the Computer Security Act of 1987 and National Security Directive 42, with the leadership responsibilities of the Commerce and De-

[56] *Federal Register* vol. 50, Dec. 24, 1985, pp. 52730-52751

[57] For applications security. agencies were required to establish management control processes to ensure appropriate security measures were implemented: agency officials were required to test security safeguards and certify they met all applicable federal requirements and standards, and agencies were required to develop and assign responsibil i ties for contingency plans. In the area of personnel security. agencies were required to establ ish screen ing procedures commensurate with the nature of the information to he handled and the potential risks and damages. Regarding installation security. agencies were required to assign responsibility for security and to conduct periodic risk analyses and establish disaster recovery and continuity plans. Agencies were also required to include all appropriate security requirements in procurement specifications for information technology" equipment, software, and services. Final l), agencies were required to establish a security awareness and training program.

fense Departments set according to whether the information domain was outside or within the area of "national security." [58]

OMB Circular A-130 was revised in 1993, but the revised version of the security appendix was not available as this report went to press. Appendix III ("Security of Federal Automated Information Systems") was being revised to incorporate requirements of the Computer Security Act of 1987 requirements for security plans described in OMB Bulletin 90-08. According to OMB, these revisions will incorporate changes based on the experience gained in visits to major agencies, and OMB will work with NIST to incorporate recommendations regarding better coordination between the Circular A-130-Revised and OMB Circular A-123.[59] With respect to safeguarding information, Circular A-130-Revised (1993) generally provides that agencies shall:

1. ensure that information is protected commensurate with the risk and magnitude of the harm that would result from the loss, misuse, or unauthorized access to or modification of such information;
2. limit the collection of information that identifies individuals only to that which is legally authorized and necessary for the proper performance of agency functions;
3. limit the sharing of information that identifies individuals or contains proprietary information to that which is legally authorized, and impose appropriate conditions on use where a continuing obligation to ensure the confidentiality of the information exists; and
4. provide individuals, upon request, access to records maintained about them in Privacy Act systems of records, and permit them to amend those records that are in error, consistent with the provisions of the Privacy Act.[60]

## The Computer Security Act of 1987

The Computer Security Act of 1987 (Public Law 100-235)[61] was a legislative response to overlapping responsibilities for computer security among several federal agencies, heightened awareness of computer-security issues, and concern over how best to control information in computerized or networked form. The act established a federal government computer security program that would protect all sensitive, but unclassified information in federal government computer systems, as well as establish standards and guidelines

---

58 The Computer Security Act of 1987 gave Commerce responsibility in information domains that contained information that was "sensitive" but not classified for national-security purposes. National Security Directive 42 ("National Policy for the Security of National *Security* [emphasis added] Telecommunications and Information Systems," July 5, 1990) established a National Security Telecommunications and Information Systems Security Committee (NSTISSC), made the Secretary of Defense the Executive Agent of the Government for National Security Telecommunications and Information Systems, and designated the Director of NSA as the National Manager for National Security Telecommunications and Information Systems.

59 of ffice of Management and Budget, "Revision of OMB Circular No. A- 130" (Plans for Development of Other Topics), *Federal Register*, vol. 58, July 2, 1993.

60 Office of Management and Budget, *Management of Federal Information Resources*, Circular A-130-Revised, June 25, 1993, sec. 8-a(9). The Secretary of Commerce is charged with developing and issuing FIPS and guidelines necessary to ensure the efficient and effective acquisition, management, and security of information technology. The Secretary of Defense is charged with developing, in consultation with the Administrator of General Services, uniform federal telecommunications standards and guidelines to ensure national security, emergency preparedness, and continuity of government (ibid., sec. 9-c,d).

61 IO I Stat. 1724. See legislative history in box 4-6.

to facilitate such protection.[62] (For legislative history of the Computer Security Act of 1987, see box 4-6.)

Specifically, the Computer Security Act assigns NBS (now NIST) responsibility for the development of government-wide computer-system security standards and guidelines, and training programs. The act also establishes a Computer System Security and Privacy Advisory Board within the Department of Commerce, and requires Commerce to promulgate regulations based on NIST guidelines. Additionally, the act requires federal agencies to identify computer systems containing sensitive information, to develop security plans for identified systems, and to provide computer security training for all employees using or managing federal computer systems. (The Computer Security Act, as well as a memorandum of understanding (MOU) between NIST and NSA and subsequent letters of clarification, is contained in appendix B of this report.)

Congressional concerns and public awareness created a climate conducive to passage of the Computer Security Act of 1987. Highly publicized incidents of unauthorized users, or "hackers," gaining access to computer systems and a growing realization of the government dependence on information technologies renewed national interest in computer security in the early 1980s.[63]

Disputes over how to control unclassified information also prompted passage of the act. The Reagan Administration had sought to give the National Security Agency much control over "sensitive, but unclassified" information, while the public-especially the academic, banking, and business communities—viewed NSA as an inappropriate agency for such responsibility. The Reagan Administration favored an expanded concept of national security.[64] This expanded concept was embodied in subsequent presidential policy directives (see below), which in turn expanded NSA's control over computer security. Questions regarding the role of NSA in security for unclassified information, the types of information requiring protection, and the general amount of security needed, all divided the Reagan Administration and the scientific community in the 1980s.[65]

### Agency Responsibilities Before the Act

Some level of federal computer-security responsibility rests with the Office of Management and Budget, the General Services Administration, and the Commerce Department (specifically NIST and the National Telecommunications and In-

62 The act was "[t]o 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" (ibid.). The National Bureau of Standards is now the National Institute of Standards and Technology.

63 U. S Congress, Office of Technology Assessment, *Federal Government Information Technology: Management, Security and COnXreSsional Oversight*, OTA-CIT-297 (Washington, DC: U.S. Government Printing Office, February 1986), pp. 64-65.

64 See e.g., Harold Relyea, *Silencing Science: National Security Controls and Scientific Communication* (Norwood, NJ: Ablex, 1994); and OTA, op. cit., footnote 1, ch. 6 and ch. 7.

65 See e.g., John T. Soma and Elizabeth J. Bedient, "Computer Security and the Protection of Sensitive but Not Classified Data: The Computer Security Act of 1987," 30 *Air Force Law Review* 135 *(1989).*

## BOX 4-6: Computer Security Act of 1987 Legislative History

In 1985, Representative Dan Glickman introduced the Computer Security and Training Act of 1985 (H.R. 2889) H.R. 2889 included provisions to establish a computer security research program within the National Bureau of Standards (now the National Institute of Standards and Technology) and to require federal agencies to train their employees and contractor personnel in computer security techniques, with the intent of establishing NBS as the developer of training guidelines for federal employees who manage, operate, or use automated information processing systems that do not include classified information.[1] Congressional hearings were held on the bill, and at the end of the 99th Congress it reached the House floor and was brought up under a suspension of the rules, but failed to obtain the two-thirds vote required and went no further.[2] In 1987, Representative Glickman, on behalf of himself and seven cosponsors, introduced H.R. 145, the Computer Security Act of 1987, based on the earlier H.R. 2889 The bill eventually had 11 cosponsors in the House,

Witnesses at hearings on H.R. 145 raised concerns over the implications of *National Telecommunications and Information Systems Security Policy Directive No.* 2, which proposed a new definition of "sensitive, but unclassified reformation."[3] This directive defined sensitive, but unclassified information as "information the disclosure, loss, misuse, alteration, or destruction of which could adversely affect national security or other federal government interests."[4] (The National Security Adviser rescinded this directive in 1987, in response to H.R. 1455, Witnesses at hearings on H.R. 145 warned that the National Security Agency could apply the "sensitive but unclassified" categorization to commercial databanks providing Information on federal government laws and policies.[6] Opponents to NSA's role in computer security also expressed concern that NSA was the agency responsible for determining federal computer systems security policy, even for systems that did not contain classified information [7] Witnesses reminded Congress that current statutes already protected proprietary and classified information and trade secrets, NSA's role in this area, therefore, was unnecessary and could lead to restrictions on access to information [8]

Congress's primary objective in enacting the Computer Security Act of 1987 was to protect information in federal computer systems from unauthorized use [9] The act set forth a clear definition of *sensitive*

---

[1] H R 2889, 99th Cong (1985) See also U S Congress, House of Representatives, *Compiler Security Act of 1987—Report to Accompany R* 145, H Rpt 10-153, 100th Cong , 1 stSess , Parts I and II (Washington, DC U S Government Printing Office, 1987), Part 1, p 8.

[2] H Rpt 100-153, op cit , footnote 1, part I, p 8,

[3] "National Policy on protection of Sensitive, but Unclassified Information in Federal Government Telecommunications and Automated Information Systems, " *National Telecommunications and Information* Systems *Security Policy Directive No* 2, Oct 29, 1986 This directive was usually referred to as NTISSP No 2

[4] Ibid , p 2

[5] H Rpt No 100-153, op cit , fOOtnOte 1, part I, p 8

[6] *Computer Security Act of 1987 Hearings on H R. 145 Be fore the Subcommittee on Legislation and National Security of the House Committee on Government Operations,* 100th Cong , Ist Sess , Feb 25, 26 and Mar 17, 1987

[7] Hearings, Committee on Government Operations, op. cit , footnote 6, P 1

[8] See *Computer Security Act of 1987 Hearings on H R. 145 Before the Subcommittee on Science, Research, and Technology and the Subcommittee on Transportation, Aviation, and Materials of the House Committee on Science, Space and Technology* 100th Cong , 1st Sess , Feb 26 and May 19, 1987

[9] H Rpt 100-153, op cit , footnote 1, Part I, P 23

*(continued)*

## BOX 4-6 (cont'd.): Computer Security Act of 1987 Legislative History

*reformation* to ease some of the concern that led to the act's passage [10] The legislative history assures that the definition of sensitive information was set forth in the Computer Security Act to guide NBS in determining what kinds of information should be addressed in its standards development process, the definition was not provided to authorize the establishment of a new quasi-classification of Information.[11]

The act's legislative history clearly Indicates that it was passed with the purpose of rejecting the federal computer security plan of *National Security Decision Directive* 145 (NSDD-145).[12] As expressed by Senator Patrick Leahy during consideration of the Act, "[NSDD-145] signaled a dramatic shift in the management of government information protection from civilian authority to military authority It has set the government on a course that has served neither the needs of national security nor the interests of the American people."[13] The Computer Security Act was intended to change the direction of this course and delegate control of unclassified Information security to the appropriate civilian agency, NBS

While Congress clearly Intended NSA to have an advisory role in all federal computer security, NBS was to have the primary role in security for unclassified information "The bill appropriately divides responsibility for developing computer security standards between the National Bureau of Standards [now NIST] and the National Security Agency NSA will provide guidelines for computer systems which handle classified information and NBS will provide guidelines for those which handle unclassified but sensitive information."[14]

Off Ice of Management and Budget Director Jim Miller stated that "it is the [Reagan] Administration's position that NBS, in developing Federal standards for the security of computers, shall draw upon technical security guidelines developed by NSA in so far as they are available and consistent with the requirements of civil departments and agencies to protect data processed in their systems When developing technical security guidelines, NSA will consult with NBS to determine how its efforts can best support such requirements In this regard the technical security guidelines provided by NSA to NBS will be treated as advisory and subject to appropriate NBS review."[15] During consideration of the act Senator Leahy said he believed that Miller's assertion continued to be the [Reagan] Administration's position and that the act would appropriately legislate such a relationship.[16] (See discussion of implementation of the Computer Security Act of 1987 and the NIST/NSA Memorandum of Understanding later in this chapter)

### Congressional Reports

- House Report 99-753 on H R 2889, "Computer Security Act of 1986, " Aug. 6, 1986
- House Report 100-153 on H R 145, "Computer Security Act of 1987, " June 11, 1987

---

10 Computer Security Act of 1987 (Public law 100-235) sec 3 *Sensitive information* was defined as "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 (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 (Ibid )

11 H Rpt 1()().153 Op cit footnote 1 Part I. p 4

12 *Congressional Record* Dec 211987. P 37679

13 Ibid

14 Ibid p 37680 (remarks of Senator William V Roth Jr)

15 H Rpt 100-153 op cit footnote 1, part I p 41 (letter to Chairman Roe), ibid part II. P 37 (letter to Chairman Brooks)

16 *Congressional Record,* Dec 21.1987 PP 3767980

*(continued)*

## BOX 4-6 (cont'd.): Computer Security Act of 1987 Legislative History

**Hearings**

- House of Representatives, Committee on Science, Space, and Technology, Subcommittee on Transportation, Aviation, and Materials, *Computerland Communications Security and Privacy,* hearing, Sept. 24, 1984
- House of Representatives, Committee on Science, Space, and Technology, Subcommittee on Transportation, Aviation, and Materials, *Computer Security Policies,* hearing, June 27, 1985.
- House of Representatives, Committee on Government Operations, Subcommittee on Legislation and National Security, *Computer Security Research and Training Act of 1985,* hearing, Sept. 18, 1985.
- House of Representatives, Committee on Government Operations, Subcommittee on Government information, Justice, and Agriculture, *Electronic Collection and Dissemination of Information by Federal Agencies,* hearings, Apr. 29, June 26, and Oct. 18, 1985
- House of Representatives, Committee on Science, Space, and Technology, Subcommittee on Transportation, Aviation, and Materials, *Federal Government Computer Security,* hearings, Oct. 29,30, 1985
- House Report 96-1540, "Government's Classification of Private Ideas, " Dec. 22, 1980.
- House of Representatives, Committee on Government Operations, Subcommittee on Legislation and National Security, *Computer Security Act of 1987,* hearings, Feb. 25, 26, Mar. 17, 1987
- House of Representatives, Committee on Science, Space, and Technology, Subcommittee on Science, Research, and Technology and Subcommittee on Transportation, Aviation, and Materials, *Computer Security Act of 1987,* hearing, Feb. 26, 1987
- House of Representatives, Committee on Science, Space, and Technology, Subcommittee on Transportation, Aviation, and Materials, *GAO Survey "Federal Government Computer Security,"* hearing, May 19, 1987

SOURCE Off Ice of Technology Assessment, 1994 and cited sources

formation Administration (NTIA)). OMB maintains overall responsibility for computer security policy.[66] GSA issues regulations for physical security of computer facilities and oversees technological and fiscal specifications for security hardware and software.[67] In addition to its other responsibilities, NSA traditionally has been responsible for security of information that is classified for national-security purposes, including Department of Defense information.[68] Under the Brooks Act, the Department of Commerce develops the Federal Information Processing Standards that provide specific codes, languages, procedures, and techniques for use by federal information systems managers.[69] NTIA serves as the Executive Branch developer of federal telecommunications policy.[70]

These overlapping agency responsibilities hindered the development of one uniform federal

66 U.S. Congress, House of Representatives, Committee on Science, Space, and Technology, *Computer Security Act of 1987—Report to Accompany H.R. /45,* H. Rept. 100-153, Part I, 100th Cong., 1 st sess., June 11, 1987 (Washington, DC: U.S. Government Printing Office, 1987), p. 7.

67 Ibid.

68 Ibid.

*69 Ibid* The FIPS apply only to federal agencies, but some, like the DES, have been adopted in voluntary standards and are used in the private sector. The FIPS are developed by NIST and approved by the Secretary of Commerce.

70 Ibid.

policy regarding the security of unclassified information, particularly because computer security and communications security historically have developed separately.[71] In 1978, OMB had issued Transmittal Memorandum No. 1 (TM-1) to its Circular A-7 1, which addressed the management of federal information technology.[72] TM-1 required federal agencies to implement computer security programs, but a 1982 GAO report concluded that Circular A-71 (and its TM-1 ) had failed to:

1. provide clear guidance to agencies on minimum safeguard requirements,
2. clarify the relationship between national-security information security and other types of information security, and
3. provide guidance on general telecommunications security.[73]

Executive orders in the 1980s, specifically the September 1984 National Security Decision Directive 145, *National Policy on Telecommunications and Automated Information Systems Security* (NSDD-145),[74] created significant shifts and overlaps in agency responsibilities. Resolving these was an important objective of the Computer Security Act. NSDD-145 addressed safeguards for federal systems that process or communicate unclassified, but "sensitive," information. NSDD-145 established a Systems Security Steering Group to oversee the directive and its implementation, and an interagency National Telecommunications and Information Systems Security Committee (NTISSC) to guide implementation under the direction of the steering group.[75]

### *Expanded NSA Responsibilities Under NSDD-145*

In 1980, Executive Order 12333 had designated the Secretary of Defense as Executive Agent of the Government for Communications Security. NSDD-145 expanded this role to encompass telecommunications and information systems security and responsibility for implementing policies developed by NTISSC. The Director of NSA was designated National Manager for Telecommunications and Automated Information Systems Security. The national manager was to implement the Secretary of Defense's responsibilities under NSDD-145. As a result, NSA was charged with examining government information and telecommunications systems to evaluate their vulnerabilities, as well as with reviewing and approving all standards, techniques, systems, and equipment for telecommunications and information systems security.

In 1985, the Office of Management and Budget (OMB) issued another circular concerning computer security. This OMB Circular A- 130, *Management of Federal Information Resources,* revised and superseded Circular A-71 (see previous section). OMB Circular A-130 defined security, encouraged agencies to consider information security essential to internal control reviews, and clarified the definition of "sensitive" information to include information "whose improper use or

---

71 I Jelenop.cit., footnote 34,pp. I.&_ H 7. Jelen explains that computer security and communications security are interdependent and inseparable because computers and telecommunications themselves converged (ibid., p. 1-7).

72 Office of Management and Budget, Transmittal Memorandum No. 1 to OMB Circular A-71, 1978.

73 U. S General Accounting Office, *Federal Information Systems Remain Highly Vulnerable to Fraudulent, Wasteful, Abusive, and Illegal Practices* (Washington, DC: U.S. Government Printing Office, 1982).

74 NSDD-145 is classified. A" unclassified version was used as the basis for this discussion.

75 This is now the National Security Telecommunications and Information Systems Security Committee, or NSTISSC. See footnote 58.

disclosure could adversely affect the ability of an agency to accomplish its mission . . . . "[76]

In 1986, presidential National Security Adviser John Poindexter[77] issued *National Telecommunications and Information Systems Security Policy Directive No. 2* (NTISSP No. 2). NTISSP No. 2 proposed a new definition of "sensitive but unclassified information." It potentially could have restricted access to information that previously had been available to the public. Specifically, "sensitive but unclassified information," within the meaning set forth in the directive, included not only information which, if revealed, could adversely affect national security, but also information that could adversely affect "other federal government interests" if released. Other federal government interests included economic, financial, technological, industrial, agricultural, and law enforcement interests.

Such an inclusive directive sparked enormous, negative public response. As the Deputy Director of NBS stated during 1987 hearings on the Computer Security Act, the NTISSP No. 2 definition of sensitive information was a ● 'totally inclusionary definition. . . [t]here is no data that anyone would spend money on that is not covered by that definition."[78] Opponents of NSDD-145 and NTISSP No. 2 argued that NSA should not have control over federal computer security systems that did not contain classified information.[79] The business community, in particular, expressed concern about NSA's ability and suitability to meet the private sector's needs and hesitated to adopt NSA's encryption technology in lieu of the DES. At the time, the DES was up for recertification.[80] In the House Report accompanying H.R. 145, the Committee on Science, Space and Technology noted that:

> NSDD-145 can be interpreted to give the national security community too great a role in setting computer security standards for civil agencies. Although the [Reagan] Administration has indicated its intention to address this issue, the Committee felt it is important to pursue a legislative remedy to establish a civilian authority to develop standards relating to sensitive, but unclassified data.[81]

In its explanation of the bill, the committee also noted that:

> One reason for the assignment of responsibility to NBS for developing federal computer system security standards and guidelines for sensitive information derives from the committee's concern about the implementation of National Security Decision Directive- 145.
>
> . . . While supporting the need for a focal point to deal with the government computer security problem, the Committee is concerned about the perception that the NTISSC favors military and intelligence agencies. It is also concerned about how broadly NTISSC might interpret its authority over "other sensitive national security information." For this reason, H.R. 145 creates a civilian counterpart, within NBS, for setting

---

76 Office of Management and Budget, OMB Circular A-130 ( 1985). As this report went to press, the computer security sections Of A-130 were still being revised but were expected to issue in 1994. The other sections of A-130 have been revised and were issued in 1993.

77 Adm. Poindexter was also chairman of the NSDD-145 Systems Security Steering Group (NSDD-145, sec. 4).

78 Raymond Kammer, Deputy Director, National Bureau of Standards, testimony, *Computer Security Act of 1987: Hearings on H.R.145 Before the Subcommittee on Legislation and National Security of the House Committee on Government Operations,* 100th Cong., 1st Sess., Feb. 26, 1987. See also H. Rept. 100-153, Part I, op. cit., footnote 66, p. 18.

79 See U.S. Congress, House Of Representatives, Committee on Science, Space and Technology, *Computer Security Act of 1987: Hearings on H.R. 145 Before the Subcommittee on Science, Research, and Technology and/he Subcommittee on Transportation, Aviation, and Materials of the House Committee on Science, Space, and Technology,* 100th Cong., 1 stsess. (Washington, DC: U.S. Government Printing Office, 198 7), pp. 146-191.

80 For history, see OTA, op. cit., footnote 1, pp. 102-108. Despite NSA's desire to replace the DES with a family of cryptographic modules using classified algorithms, it was reaffirmed in 1988.

81 H. Rept. 100-153, Part ], op. cit., footnote 66, p. 22.

> policy with regard to unclassified information... NBS is required to work closely with other agencies and institutions such as NSA, both to avoid duplication and to assure that its standards and guidelines are consistent and compatible with standards and guidelines developed for classified systems; but the final authority for developing the standards and guidelines for sensitive information rests with the NBS.[82]

In its report on H.R. 145, the Committee on Government Operations explicitly noted that the bill was ● 'neutral" with respect to public disclosure of information and was not to be used by agencies to exercise control over privately owned information, public domain information, or information disc losable under the Freedom of Information Act or other laws.[83] Furthermore, the committee noted that H.R. 145 was developed in large part to ensure the delicate balance between "the need to protect national security and the need to pursue the promise that the intellectual genius of America offers us." 84 The committee also noted that:

> Since it is a natural tendency of DOD to restrict access to information through the classification process, it would be almost impossible for the Department to strike an objective balance between the need to safeguard information and the need to maintain the free exchange of information.[85]

Subsequent to the Computer Security Act of 1987, DOD's responsibilities under NSDD-145 were aligned by National Security Directive 42 (NSD 42) to cover "national security" telecommunications and information systems.[86] NSD 42 established the National Security Telecommunications and Information Systems Security Committee (NSTISSC), made the Secretary of Defense the Executive Agent of the Government for National Security Telecommunications and Information Systems, and designated the Director of NSA the National Manager for National Security Telecommunications and Information Systems.[87] As such, the NSA director is to coordinate with NIST in accordance with the Computer Security Act of 1987. NSD 42 does not rescind programs, such as those begun under NSDD-145, that pertain to national-security systems, but these are not construed as applying to systems within the purview of the Computer Security Act of 1987.88

### *Agency Information-System Security Responsibilities Under the Act*

Under the Computer Security Act of 1987, all federal agencies are required to identify computer systems containing sensitive information, and to develop security plans for identified systems.[89] The act also requires mandatory periodic training in computer security for all federal employees and contractors who manage or use federal computer systems. **The Computer Security Act gives final authority to NIST [then NBS] for developing government-wide standards and guidelines for unclassified, sensitive information, and for developing government-wide training programs.**

In carrying out these responsibilities, NIST can draw upon the substantial expertise of NSA and other relevant agencies. Specifically, NIST is

---

82 Ibid., p. 26.

83 H. Rept. 100.1 53, Part 11, op. cit., footnote 33, p. 30.

84 Ibid., p. 29.

85 Ibid., p. 29.

86 National Security Directive 42, op. cit., footnote 58. The National Security Council released an unclassified, partial text of NSD 42 to the Computer l%) )fessionals for Social Responsibility on Apr. 1, 1992, in response to Freedom of Information Act (FOIA) requests made in 1990.

87 NSD 42 (unclassified partial text), sees.l -7

88 Ibid,, sec. 10.

89 Public Law 100-235, sec. 6.

COURTESY NATIONAL SECURITY AGENCY

*The National Cryptologic Museum at Ft. George G Meade, Maryland*

authorized to “coordinate closely with other agencies and offices” including NSA, OTA, DOD, the Department of Energy, GAO, and OMB.[90] This coordination is aimed at “assur[ing] maximum use of all existing and planned programs, materials, studies, and reports relating to computer systems security and privacy” and assuring that NIST’s computer security standards 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.”[91] Additionally, the Computer Security Act authorizes NIST to “draw upon computer system technical security guidelines developed by [NSA] to the extent that [NIST] determines that such guidelines are consistent with the requirements for protecting sensitive information in federal computer systems.’’[92] The act expected that "[t]he method for promulgating federal computer system security standards and guidelines is the same as for non-security

[90] I bid., wc. 3(b)(6). NIST coordination with OTA in this regard generally consists of including OTA staff in external review of selected NIST reports.

[91] Ibid.

[92] Ibid.

standards and guidelines." 93 The intent of the act was that NSA not have the dominant role and to recognize the potential market impact of federal security standards:

> . . . [I]n carrying out its responsibilities to develop standards and guidelines for protecting sensitive information in federal computer systems and to perform research, NBS [now NIST] is required to draw upon technical security guidelines developed by the NSA to the extent that NBS determines that NSA's guidelines are consistent with the requirements of civil agencies. The purpose of this language is to prevent unnecessary duplication and promote the highest degree of cooperation between these two agencies. NBS will treat NSA technical security guidelines as advisory, however, and, in cases where civil agency needs will best be served by standards that are not consistent with NSA guidelines, NBS may develop standards that best satisfy the agencies' needs.
>
> It is important to note the computer security standards and guidelines developed pursuant to H.R. 145 are intended to protect sensitive information in Federal computer systems. Nevertheless, these standards and guidelines will strongly influence security measures implemented in the private sector. For this reason, NBS should consider the effect of its standards on the ability of U.S. computer system manufacturers to remain competitive in the international marketplace.[94]

In its report accompanying H.R. 145, the Committee on Government Operations noted that:

> While the Committee was considering H.R. 145, proposals were made to modify the bill to give NSA effective control over the computer standards program. The proposals would have charged NSA with the task of developing "technical guidelines," and forced NBS to use these guidelines in issuing standards.
>
> 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 most of the program—the technical guidelines developed by NSA.
>
> This would jeopardize the entire Federal standards program. The development of standards requires interaction with many segments of our society, i.e., government agencies, computer and communications industry, international organizations, etc. NBS has performed this kind of activity very well over the last 22 years [since enactment of the Brooks Act of 1965]. NSA, on the other hand, is unfamiliar with it. Further, NSA's products may not be useful to civilian agencies and, in that case, NBS would have no alternative but to issue standards based on these products or issue no standards at all.[95]

The Committee on Government Operations also noted the concerns of industry and the research community regarding the effects of export controls and NSA involvement in private-sector activities, including restraint of innovation in cryptography resulting from reduced incentives for the private sector to invest in independent re-

93 H.Rept.100-153, Part 1, op. cit., footnote 66, p. 26.

94 Ibid., p. 27.

95 H.Rept.100-153, Part II, op. cit., footnote 33, pp. 25-26.

search, development, and production of products incorporating cryptography.[96]

The Computer Security Act of 1987 established a Computer System Security and Privacy Advisory Board (CSSPAB) within the Department of Commerce:

> The chief purpose of the Board is to assure that NBS receives qualified input from those likely to be affected by its standards and guidelines, both in government and the private sector. Specifically, the duties of the Board are to identify emerging managerial, technical, administrative and physical safeguard issues relative to computer systems security and privacy and to advise the NBS and the Secretary of Commerce on security and privacy issues pertaining to federal computer systems.[97]

The Chair of the CSSPAB is appointed by the Secretary of Commerce. The board is required to report its findings relating to computer systems security and privacy to the Secretary of Commerce, the OMB Director, the NSA Director, the House Committee on Government Operations, and the Senate Committee on Governmental Affairs.[98]

Implementation of the Computer Security Act has been controversial, particularly with respect to the roles of NIST and NSA in standards development. The two agencies developed a memorandum of understanding to clarify the working relationship, but this MOU has been controversial as well, because of concerns in Congress and elsewhere that its provisions cede NSA much more authority than the act had granted or envisioned.[99] The last section in this chapter examines implementation issues related to the MOU and the roles of NIST and NSA. (Chapter 2 examined additional implementation issues concerning the federal role in safeguarding information in the information infrastructure.)

## Future Directions in Safeguarding Information In Federal Agencies

Information resource management in the federal government is in need of general reform. Information technologies—properly used—have the potential not only to improve government information resource management, but also to improve the overall effectiveness and efficiency of government.[100] This requires that top management is informed and interested—information technology has all too often been viewed as a tool to make incremental improvements, rather than an integral part of operations. Compared with traditional mainframe or paper-based methods, modern databases and networking services provide opportunities to actually change the way that fed-

---

96 Ibid., pp. 22.25 and 30.35. In 1986, NSA had announced a program to develop cryptographic modules that qualified communications manufacturers could embed in their products. NSA's development of these embeddable modules was part of NSA's Development Center for Embedded COMSEC Products. (NSA Press release for Development Center for Embedded COMSEC products, Jan. 10, 1986.)

97 H. Rept. 100-153, Part 1, op. cit., footnote 66, pp. 27-28.

98 Public Law 100-235, sec. 3.

99 The manner in which NIST and NSA planned to execute their functions under the Computer Security Act of 1987, as evidenced by the MOU, was the subject of hearings in 1989. See U.S. Congress, House of Representatives, Subcommittee on Legislation and National Security, Committee on Government Operations, *Military and Civilian Control of Computer Security Issues*, 101 st Cong., 1 st sess., May 4, 1989 (Washington, DC: U.S. Government Printing Office, 1989). The NIST-NSA working relationship has subsequently been raised as an issue, with regard to the EES and the DSS.

100 See Committee on Applications and Technology, National Information Infrastructure Task Force, *Putting the Information Infrastructure to Work*, NIST Special Publication 857 (Washington, DC: U.S. Government Printing Office, May 1994).

eral agencies (as well as corporations and other organizations) do business. [101]

Clear, strong leadership is vital to effective use of information technology. [102] Leadership and management commitment are also crucial in safeguarding information. [103] Unfortunately, responsibility for information safeguards has often been disconnected from the rest of information management, and from top management. Information safeguards have all too often been viewed as expensive overhead, rather than a valuable form of insurance. Higher level agency managers are not necessarily unconcerned about protecting the organization's assets, but are under constant pressure to trim budgets and personnel. Responsibility y for information safeguards too often lies with computer security professionals who do not have the authority and resources they need.

This disconnected responsibility is not limited to the federal government. Information safeguards generally tend not to be addressed with the levels of attention they deserve, even in the private sector, One reason may be that the field of information safeguards is relatively new and lacks the historical development and popular attention that exist in older fields, such as airplane or bridge safety. [104] Problems due to an absence or breakdown of information safeguards can be underreported, or even kept completely secret. Information-security "disasters," "near misses," and compromises, like the 1988 Internet Worm and the 1994 ''password sniffer" network monitoring incidents and intrusions into civilian and military computer systems, have only recently begun to receive popular attention. [105]

The Computer Security Act of 1987 requires all federal agencies to identify computer systems containing sensitive information, and to develop security plans for these systems. [106] The act also requires mandatory periodic training in computer security for all federal employees and contractors who manage, use, or operate federal computer systems. In its workshops and discussions with federal employees and knowledgeable outside observers, OTA found that these provisions of the Computer Security Act are viewed as generally

---

101 Reforming information resource management in the federal government to improve electronic delivery of services is discussed in U.S. Congress, Office of Technology Assessment, *Making Government Work: Electronic Delivery of Federal Services*, OTA-TCT-578 (Washington, DC: U.S. Government Printing Office, September 1993). See also Office of the Vice President, *Reengineering Through Information Technology (Accompanying Report of the National Performance Review)*, September 1993 (released May 1994).

102 See U.S *Genera] Accounting Office, Executive Guide: Improving Mission Performance Through Strategic Information Managment and* Technology, GAO~AIMD-94-115 (Washington, DC: U.S. Government Printing Office, May 1994). See also *Reengineering Through Information Technology),* op. cit., footnote 101, ch. IT01.

103 Ibid., ch. IT I 0.

104 Computer models to simulate and test bridge and airplane designs have been used for decades. A sensational airplane or bridge disaster is also obvious, and ascertaining accountability is generally more straightforward. In contrast, networks are changing constantly. No good methodology exists to prove that a network is secure, or to simulate its operation under worst-case conditions.

105 See peter H. Lewis, ' Hackers on Internet posing Security Risks, Experts Say," The *New York Times*, July 21, 1994, pp. 1, B 10. See also L. Dain Gary, Manager, Computer Emergency Response Team Operations, Carnegie Mellon University, testimony, *Hearing on Internet Security*. Subcommittee on Science, Committee on Science, Space, and Technology, U.S. House of Representatives, Mar. 22, 1994; and F. Lynn McNulty, NIST Associate Director for Computer Security, testimony, *Hearing on Internet Security*, Subcommittee on Science, Committee on Science, Space, and Technology, U.S. House of Representatives, Mar. 22, 1994.

106 Public Law 100-235, SeC. 6.

adequate as written, but that their implementation can be problematic.[107]

During the course of this project, OTA found strong sentiment that agencies follow the rules set forth by the Computer Security Act, but not necessarily the full intent of the act. In practice, there are both insufficient incentives for compliance and insufficient sanctions for noncompliance with the spirit of the act—for example, agencies do develop the required security plans. However, the act does not require agencies to review them periodically or update them as technologies or circumstances change. One result of this is that "[security of systems tends to atrophy over time unless there is a stimulus to remind agencies of its importance."[108] Another result is that agencies may not treat security as an integral component when new systems are being designed and developed.

OMB is responsible for developing and implementing government-wide policies for information resource management; for overseeing the development and promoting the use of government information-management principles, standards, and guidelines; and for evaluating the adequacy and efficiency of agency information-management practices. Information-security managers in federal agencies must compete for resources and support to properly implement needed safeguards. In order for their efforts to succeed, both OMB and top agency management must fully support investments in cost-effective safeguards. Given the expected increase in interagency sharing of data, interagency coordination of privacy and security policies is also necessary to ensure uniformly adequate protection.

The forthcoming revision of Appendix III ("Agency Security Plans") of OMB Circular A-130 will be central to improved federal information security practices. The revision of Appendix 111 will take into account the provisions and intent of the Computer Security Act, as well as observations regarding agency security plans and practices that resulted from series of agency visits made by OMB, NIST, and NSA in 1992. 'W Because the revised Appendix III had not been issued at the time this report was written, OTA was unable to gauge its potential for improving information security in federal agencies or its potential for making implementation of the Computer Security Act more effective. To the extent that the revised Appendix 111 facilitates more uniform treatment across federal agencies, it can also make fulfillment of Computer Security Act and Privacy Act requirements more effective when agencies share data (see chapter 3).

## U.S. EXPORT CONTROLS ON CRYPTOGRAPHY

The United States has two regulatory regimes for exports, depending on whether the item to be exported is military in nature, or is "dual-use," having both civilian and military uses. These regimes are administered by the State Department and the Commerce Department, respectively. Both rc-

---

107 Some of the possible measures to improve implementation that were suggested during these discussions were: increasing resources for OMB to coordinate and oversee agency security plans and training; increasing resources for NIST and/or other agencies to advise and review agency security plans and training; setting aside pan of agency budgets for information security (to be used for risk assessment, training, development, and so forth); and/or rating agencies according to the adequacy and effectiveness of their information-security policies and plans and withholding funds until performance meets predetermined accepted levels. (Discussions in OTA workshops and interviews, 1993 -94.)

108 Office of Management and Budget (in conjunction with NIST and NSA), *Observations of Agency Computer Security Practices and Implementation of OMB Bulletin No. 90-08: Guidance for Preparation of Security Plans for Federal Computer Systems That Contain Sensitive Information*, February 1993, p. 11.

109 Ibid. According to OMB, NIST, and NSA, these visits were successful in raising agency managers' awareness of Computer security and of its importance. The three agencies found that periodically focusing senior management attention on the value of computer security to agency operations and service delivery improves the effectiveness of agency computer security programs and can also result in increased resources and updated security policy directives (pp. 1 I - 12).

gimes provide export controls on selected goods or technologies for reasons of national security or foreign policy. Licenses are required to export products, services, or scientific and technical data[110] originating in the United States, or to re-export these from another country.

Licensing requirements vary according to the nature of the item to be exported, the end use, the end user, and, in some cases, the intended destination. For many items, no specific approval is required and a "general license" applies (e.g., when the item in question is not military or dual-use and/or is widely available from foreign sources). In other cases, an export license must be applied for from either the State Department or the Commerce Department, depending on the nature of the item. In general, the State Department's licensing requirements are more stringent and broader in scope. 111 Licensing terms differ between the agencies, as do time frames and procedures for licensing review, revocation, and appeal.

## State Department Export Controls on Cryptography

The Arms Export Control Act and International Traffic in Arms Regulations(ITAR)112 are administered by the State Department and control export of items (including hardware, software, and technical data) that are "inherently military in character" and, therefore, placed on the Munitions List. [113] Items on the Munitions List are controlled to all destinations, meaning that "validated" licenses—requiring case-by-case review—are required for any exports (except to Canada, in some cases). The Munitions List is established by the State Department, in concurrence with the Department of Defense; the State Department Office of Defense Trade Controls administers the ITAR and issues licenses for approved exports. DOD provides technical advice to the State Department when there are questions concerning license applications or commodity jurisdiction (i.e., whether State or Commerce regulations apply—see below).

With certain exceptions, cryptography falls in '*Category XIII—Auxiliary Military Equipment" of the Munitions List. Category XIII(b) covers "Information Security Systems and equipment, cryptographic devices, software and components specifically designed or modified therefore," generally including:

1. cryptographic and key-management systems and associated equipment, subcomponents, and software capable of maintaining information or information-system secrecy/confidentiality;

---

110 Both the Export Administration Act (50 U.S.C. App. 2401-2420) and the Arms Export Control Act (22 U.S.C. 275 1-2794) provide authority to control the dissemination to foreign nationals (export) of scientific and technical data related to items requiring export licenses under the regulations implementing these acts. "Scientific and technical data" can include the plans, design specifications, or other information that describes how to produce an item.

For history and discussion of national-security controls on scientific and technical data, see H. Relyea, op. cit., footnote 64; and Kenneth Kalivoda, "'The Export Administration Act's Technical Data Regulations: Do They Violate the First Amendment?" *Georgia Journal of International and Comparative Law*; vol. 1 I, fall 1981, pp. 563-587. Other statutory authorities for national-security controls on scientific and technical data are found in the Restricted Data or "born classified" provisions of the Atomic Energy Act of 1946 (60 Stat. 755) and the Atomic Energy Act of 1954 (68 Stat. 919, 42 U.S.C. 2011-2296) and the Invention Secrecy Act of 1951 (35 U.S.C. 181-188), which allows for patent secrecy orders and withholding of patents on national-security grounds. NSA has obtained patent secrecy orders on patent applications for cryptographic equipment and algorithms under authority of the Invention Secrecy Act.

111 For a comparison of the two export-control *regimes, see* U.S. General Accounting Office, *Export Controls: Issues in Renlf~~'in/! Militarily Sensitive Items from the Munitions List*, GAO/NSIAD-93-67 (Washington, DC: U.S. Government printing Office, March 1993), especially pp. 10-13.

112 22 C.F.R. 120-130.

113 See Supplement 2 to Part 770 of the Export Administration Regulations. The Munitions List has 21 categories of items and related technologies, such as artillery and projectiles (Category 11) or toxicological and radiological agents and equipment (Category XIV). Category Xl II(b) consists of "Information Security Systems and equipment, cryptographic devices, software, and components specifically modified therefore."

2. cryptographic and key-management systems and associated equipment, subcomponents, and software capable of generating spreading or hopping codes for spread-spectrum systems or equipment;
3. cryptanalytic systems and associated equipment, subcomponents, and software;
4. systems, equipment, subcomponents and software capable of providing multilevel security that exceeds class B2 of the NSA's Trusted Computer System Evaluation Criteria, as well as software used for certification;
5. ancillary equipment specifically designed or modified for these functions; and
6. technical data and defense services related to the above. '

Several exceptions apply to the first item above. These include the following subcategories of cryptographic hardware and software:

a. those used to decrypt copy-protected software, provided that the decryption functions are not user-accessible;
b. those used only in banking or money transactions (e.g., in ATM machines and point-of-sale terminals, or for encrypting interbanking transactions);
c. those that use analog (not digital) techniques for cryptographic processing in certain applications, including facsimile equipment, restricted-audience broadcast equipment, and civil television equipment;
d. those used in personalized smart cards when the cryptography is of a type restricted for use only in applications exempted from Munitions List controls (e.g., in banking applications);
e. those limited to access-control functions (e.g., for ATM machines, point-of-sale terminals, etc.) in order to protect passwords, personal identification numbers, and the like provided that they do not provide for encryption of other files or text;
f. those limited to data authentication (e.g., calculating a message authentication code) but not allowing general file encryption;
g. those limited to receiving radio broadcast, pay television, or other consumer-type restricted audience broadcasts, where digital decryption is limited to the video, audio, or management functions and there are no digital encryption capabilities; and
h. those for soft ware designed or modified to protect against malicious computer damage from viruses, and so forth. [115]

Cryptographic hardware and software in these subcategories are excluded from the ITAR regime and fall under Commerce's jurisdiction. Note, however, that these exclusions do not include hardware-based products for encrypting data or other files prior to transmission or storage, or user-accessible, digital encryption software for ensuring email confidentiality or read-protecting stored data or text files. These remain under State Department control.

---

[114] Ibid. See Category XIII(b)((1)-(5)) and XIII(k). For a review of controversy during the 1970s and early 1980s concerning control of cryptographic publication, see F. Weingarten, "Controlling Cryptographic Publication," *Computers & Security*, vol. 2, 1983, pp. 41-48,

[115] Ibid. See XIIf(b)(1)(i)-(ix).

## Commerce Department Export Controls on Cryptography

The Export Administration Act (EAA)[116] and Export Administration Regulations (EAR) [117] are administered by the Commerce Department and are designed to control exports of "sensitive" or dual-use items, also including software and scientific and technical data. The Bureau of Export Administration administers controls on dual-use items; the Office of Export Licensing makes licensing determinations (coordinating with other agencies as necessary), and the Office of Technology and Policy Analysis develops licensing policies and provides technical support in maintaining the Commerce Control List (CCL). Some items on the CCL are controlled for national-security purposes, to prevent them from reaching "proscribed" countries (usually in the former Soviet bloc); others are controlled for various foreign policy objectives.[118]

Cryptography falls under Section 11 ("Information Security") of the CCL.[119] This category includes information-security "equipment, assemblies and components" that:

1. are designed or modified to use digital cryptography for information security;
2. are designed or modified to use cryptanalytic functions;
3. are designed or modified to use analog cryptography, except for some low-speed, fixed band scrambling or frequency inversion, or in facsimile equipment, restricted audience broadcast equipment or civil television equipment (see item c above);
4. are designed to suppress compromising emanations of information-bearing signals, except for suppression of emanations for health or safety reasons;
5. are designed or modified to use cryptography to generate the spreading code for spread-spectrum systems or the hopping code for frequency agility systems; or
6. are designed or modified to exceed class B2 of the Trusted Computer System Evaluation Criteria (see item 4 in the State Department list above); plus
7. communications cable systems with intrusion-detection capabilities.

Equipment for the test, inspection, and production (including evaluation and validation equipment) of equipment or functions in this category are included, as are related software and technology.

The "overlap" between the State Department and Commerce Department export-control regimes is particularly complex for cryptography (note the overlap between the Munitions List items and the CCL items, even with the exceptions). Basically, the Commerce Department licenses only those Section II items that are either excepted from State Department control, are not controlled, or are eligible for licensing under an advisory note, plus anti-virus software (see h

---

116 In the 103d Congress, legislation intended to streamline controls and ease restrictions on mass-market computer software, hardware, and technology, including certain encryption software, was introduced. Provisions in H.R. 3627 and S. 1846 placed mass-market software with encryption under Commerce controls. At this writing, the 1994 omnibus export administration bills (H. R. 3937 and S. 1902) were awaiting congressional action. See U. S. Congress, House of Representatives, *Omnibus Export Administration Act of* 1994, H. Rept. 103-531, 103d Cong., 2d sess., Parts 1 (Committee on Foreign Affairs, May 25, 1994), 2 (Permanent Select Committee on Intelligence, June 16, 1994), 3 (Committee on Ways and Means, June 7, 1994), and 4 (Committee on Armed Services, June 17, 1994) (Washington, DC, U.S. Government Printing Office, 1994), and H.R. 4663, "Omnibus Export Administration Act of 1994," June 28, 1994.

117 22 U.S.C. 2751-2794,

118 See GAO, op. cit., footnote 111, pp. 10-12.

119 See Supplement 1 to Part 799 1 of the Export Administration Regulations, sections A (equipment, assemblies and components), B (test, inspection, and production equipment), D (software), and E (technology).

above).[120] The cryptographic items *excepted* from control under advisory note 1 are: personalized smart cards as described in item d above; equipment for fixed data compression or coding techniques, or for use in applications described in item g above; portable, commercial civil cellular phones containing encryption, when accompanying their users; and software as described in item a above.[121] Other items, such as cellular phone systems for which message traffic encryption is not possible, or items for civilian use in banking, access control, and authentication as described under items b, e, or f above, are covered by advisory notes 3 through 5. These advisory notes state that these items are likely to be licensed by Commerce, as administrative exceptions, for export to acceptable end users.[122]

At present, however, software and hardware for robust, user-controlled encryption remains on the Munitions List under State Department control, unless State grants jurisdiction to Commerce.[123] This has become increasingly controversial, especially for the information technology and software industries. According to GAO's 1993 report:

> NSA performs the technical review that determines, for national security reasons, (1) if a product with encryption capabilities is a munitions item or a Commerce List item and (2) which munitions items with encryption capabilities may be exported. The Department of State examines the NSA determination for consistency with prior NSA determinations and may add export restrictions for foreign policy reasons—e.g., all exports to certain countries may be banned for a time period. . . . [T]he detailed criteria for these decisions are generally classified. However, vendors exporting these items can learn some of the general criteria through prior export approvals or denials they have received. NSA representatives also advise companies regarding whether products they are planning would likely be munitions items and whether they would be exportable, according to State Department representatives.[124]

## Export Controls and Market Competitiveness

The United States was a member of the Coordinating Committee for Multilateral Export Controls (COCOM), which was dissolved on March 31, 1994, The COCOM regime had an "East-West" focus on controlling exports to communist countries. Within COCOM, member nations agreed on controls for munitions, nuclear, and dual-use items. However, when U.S. export controls were more stringent than COCOM controls, U.S. firms were at a disadvantage in competing for markets abroad, relative to competitors in other COCOM countries.

After COCOM ended, the United States and its former partners set about establishing a new, multilateral regime designed to address new security threats in the post-Cold War world. '[25] Major goals for the new regime will be to deny trade in dangerous arms and sensitive technologies to particular regions of the world and to "rogue countries" such as Iran, Libya, Iraq, and North Korea.[126] The target goal for the establishment of the new multilateral regime is October 1994. Until the new regime is established, the United States

---

120 ibid,, p. CCL 123 (notes). The advisory notes specify items that can be licensed by Commerce under one or more administrative exceptions.

121 Ibid pp CCL 123.126. Software required for or providing these functions is also excepted.

122 Ibid., Advisory Notes 1-5.

123 GAO, Op. cit., footnote 48, pp. 24-28.

124 Ibid., p. 25.

125 Lynn Davis, Undersecretary for International Security Affairs, U.S. Department of State, press briefing, Apr. 7, 1994. (As this report went to press, this was the most current public information available to the OTA project staff regarding post-COCOM export regimes. )

126 Ibid.

and other partners in the discussions have agreed to continue "controls or licensing on the most sensitive items in arms" but on a global basis, rather than in an East-West context.[127] These continued controls are being implemented on a "national discretion" basis, where each nation retains the right to do as it wishes. This contrasts with the "consensus" rule under which COCOM had operated, where any state (e.g., the United States) could unilaterally block exports proposed by any other state. [128]

At the end of COCOM, the Clinton Administration liberalized the policy for some exports of computer and telecommunications products to Russia, Eastern Europe, and China. However, controls were maintained on cryptography because:

> The President has determined that vital U.S. national security and law enforcement interests compel maintaining appropriate control of encryption.[129]

The end of the Cold War and opening up of the former Soviet bloc have led to new market opportunities for U.S. firms and their competitors. Many countries—including former COCOM countries like Japan and members of the European Community, as well as others—have less restrictive export controls on encryption technology than the United States. '30 (However, some of these have import controls on encryption, which the United States does not.[131]) As a result, U.S. firms (including software companies) are pressing for a fundamental rethinking of the system of export controls. Some progress was previously made in this area, including transfer of some dual-use items formerly on the Munitions List to Commerce Department control. This "rationalization" was accomplished through a 1991-92 interagency review of items on the U.S. Munitions List to determine which of those also on COCOM's Industrial List (IL) of dual-use technologies could be removed from the ITAR regime without jeopardizing significant national-security interests. [132]

The rationalization process led to removal of over two dozen items, ranging from armored coaxial cable to several types of explosives, from the Munitions List. Some other items, however, were "contentious." These contentious items, which State and Defense identified for retention on the Munitions List, included some commercial software with encryption capability. According to GAO:

> State and Defense wanted to retain software with encryption capability on the USML [Munitions List] so the National Security Agency (NSA) can continue its current arrangement

---

127 *Ibid* ..."we've also agreed to exercise extreme *Vigilance* on a global basis for all trade in the most sensitive of these items, so that we will be continuing to control these most sensitive items not (rely to the formerly proscribed countries of Russia and China but also now around the world to include countries such as Iran." (Undersecretary Davis, ibid. )

128 See U.S. *Congress,* Office of Technology Assessment, *Export Controls* and *Nonproliferation Policy, OTA-I* SS-596 (Washington, DC U.S. Government Printing Ofice, May 1994), especially table 5-2, p. 44.

129 Martha Harris, Deputy Assistant Secretary for Political-Military Affairs, U.S. Department Of State, "Encryption-Export Control Reform," statement, Feb. 4, 1994.

130 See James P. Chandler et al. (National Intellectual Property Law Institute, The George Washington University), "identification and Analysis of Foreign Laws and Regulations Pertaining to the Use of Commercial Encryption Products for Voice and Data Communications," contractor report to the U.S. Department of Energy Under Contract No. DE-AC05-84OR2 1400, January 1994.

131 France, for example, requires a license for the import of encryption and DES-based manufacturers and users must deposit a key with the French government. China restricts both the importation and exportation of voice-encoding devices (ibid.).

132 GAO op. *Cit.,* footnote 48 pp. 9-10 and 13-15. According to the U.S. General Accounting Office, some items on the IL appeared on both the CCL and the Munitions List, when the State Department and DOD wanted to keep an item on the Munitions List after COCOM moved it to the IL. This would occur when State and DOD wanted to maintain the more restrictive International Traffic in Arms Regulations controls on militarily sensitive items for which the United States has a technological lead. Generally, though, when items were added to the IL, they were added to the CCL (ibid., p. 13).

> with industry to review all new software with encryption capability coming to market to determine if the new product should be controlled on the USML or the CCL. One reason for maintaining this item on the munitions list is concern over future encryption development by software firms being placed on commercial software programs. Additional reasons are classified. The software industry is concerned that it is losing its competitive advantage because software with encryption capability is controlled under the USML. [133]

Some other contentious items, namely nonmilitary image intensifiers and technical data associated with inertial navigation systems, were eventually transferred to the Commerce Control List by interagency agreements, with Commerce agreeing to impose additional foreign-policy controls to alleviate DOD's concerns. However, GAO found that:

> State later proposed to transfer mass-market software, including software with encryption capabilities, to Commerce's jurisdiction because it believed that it would be impossible to control such software. Defense, led by the National Security Agency, refused to include this item in any compromise with Commerce, citing the inadequacy of Commerce's control system even with added foreign policy controls. The National Security Agency was also concerned that foreign policy controls may lead to decontrol. Further, Defense cited administration opposition to a provision in a bill to reauthorize and amend the Export Administration Act as another reason that jurisdiction over software should not be transferred. The provision, if passed, would have moved all mass-market software from the USML to the CCL, including software with encryption capability. On February 3, 1992, the Acting Secretary of Commerce notified the Congress that including this provision would lead senior advisors to recommend that the President [Bush] veto the bill. Defense's argument prevailed, and the item was retained on the USML. [134]

Thus, as this report went to press, U.S. software producers still faced the ITAR restrictions for exports of software with strong encryption.[135] Software (or hardware) products using the DES for message encryption (as opposed to message authentication) are on the Munitions List and are generally nonexportable to foreign commercial users, except foreign subsidiaries of U.S. firms and some financial institutions (for use in electronic funds transfers). This means that individual, validated licenses—requiring a case-by-case review of the transaction—must be obtained for products and programs that have strong data, text, or file encryption capabilities. [136] Products that use the DES and other algorithms for purposes other than message encryption (e.g., for authentication) are exported on the Commerce Control List, however. [137]

In 1992, there had been limited relaxation of export controls for mass-marketed software with

---

133 Ibid., p. 21. GAO examined DOD's classified national-security justifications for retaining several other items (e.g., technical data for nonmilitary inertial navigation systems) and found them to be "sound." However, due to the level of classification involved, GAO did not examine the justification for retaining cryptographic software on the Munitions List (ibid., p. 19).

134 Ibid., pp. 21-22.

135 "Strong" encryption in this context refers to systems on a par with the DES or with the RSA system with a 1@24-bit modulus.

In 1992, some mass-market software with encryption (but not the DES) was moved to Commerce control, given an expedited NSA review. According to NSA, requests to move mass-market software products to Commerce have usually been granted, except for those that include the DES for data encryption. (Roger Callahan, NSA, personal communication, June 8, 1994, point 7.)

136 Under these rules, the exporting firm has to apply for a separate license for each customer (e.g., overseas subsidiary, independent software distributor, foreign computer manufacturer); a license is valid for one product. The exporter must tile annual reports listing the number of copies sold to the customer, to whom they were sold, and the sale price. (Business Software Alliance, Unrealistic U.S. Government Export Controls Limit the Ability of American Companies To Meet the Demand for Encryption," 1994. )

137 GAO, Op. cit., footnote 48, p. 26.

encryption capabilities. NSA and the State Department relaxed and streamlined export controls for mass-market software with moderate encryption capabilities, but not including software implementing the DES or computer hardware containing encryption algorithms.[138] Also, since July 1992, there has been expedited review of software using one of two algorithms developed by RSA Data Security, Inc. These algorithms, called RC2 and RC4, are said to be significantly stronger than those previously allowed for export, but are limited to a 40-bit key length and are said to be weaker' 39 than the "DES-strength" programs that can be marketed in the United States and that are available overseas.[140]

As a result of U.S. export controls, some firms have produced "U.S.-only" and "export" versions of their products; others report that overseas markets have been foreclosed to them, even as worldwide demand for data encryption is dramatically increasing.[141] Companies with offices in the United States and overseas have faced operational complications from export requirements, including a lack of integrated (as opposed to add-on) encryption products.[142] Business travelers also potentially violated ITAR by traveling abroad without licenses for mass-market software containing encryption algorithms loaded in their laptop or notebook computers. (At this writing, provisions were being put in place to allow business travelers to carry domestic encryption products overseas for personal use—see discussion of licensing reforms below.) Companies that employ foreign nationals face additional complications in licensing and end-use regulations.[143]

According to the Business Software Alliance (BSA), the net result is a "virtual embargo" to foreign commercial users of U.S. products with strong encryption (e.g., the DES).[144] Under current rules, obtaining a license to export encryption products to financial institutions can take several weeks; qualifying subsidiaries must have at least 50 percent U.S. ownership.[145] One way through these strict controls is to disable any file- or text-encryption capabilities in the "export" version.

At a May 1994 hearing before the Senate Subcommittee on Technology and the Law, Stephen Walker (Trusted Information Systems, Inc.) presented the results of SPA's study of the foreign availability of encryption products. As of April 1994, SPA reported having identified 423 U. S.-

---

138 [bId.

139 See Walker testimony, op. cit., footnote 37, p. 9.

140 Software Publishers Association, "SPA News," March 1994, p. *94.* See also Walker testimony, 0p. Cit., footnote 37, P. 28. According to a 1992 presentation by Jim B idzos (President, RSA Data Security, Inc. ) to the Computer System Security and Privacy Ad\ isory Board (CSSPAB ), RC2 and RC4 were developed by RSA Data Security, Inc. in the mid- 1980s and are not public-key based. They have been incorporated into Lotus Notes. (Minutes of the September 15-17, 1992 meeting of the CSSPAB, obtained from NIST.)

141 See Business Software Alliance (BSA), op. cit., footnote 136. According to BSA, its member companies account for 7 l *percent* of prepackaged PC software sales by U.S. companies. See also software-producer testimonies before the Subcommittee on Economic Policy. Trade and Environment, House Committee on Foreign Affairs, Oct. 12, 1993 and GAO, op. cit., footnote 48, pp. 26-28.

142 See Priscilla A Walter and Louis K. Ebling, "Taming the Jungle of Export Regulations, " *The International Computer Lawyer, vol.* 1, No. 11, October *1993,* pp. 14-16.

143 *Ibid,,* p. 16. However, according to NSA, it is not difficult to obtain licensing for an employed foreign national. (Roger Callahan, NSA, personal communication, June 8, *1994,* point 1 2.)

144 BSA op. cit., footnote 136, pp. 1-2, citin, statement by Bob Rarog, Digital Equipment Corp., before the CSSPAB, June 3, 1993.

145 Ellen Messmer "Encryption Restriction Policy Hurts Users, Vendors," *Network World,* Aug. 23, 1993, pp. 34,43. Semaphore Corp., a U.S. manufacturer of encryption products, estimated that U.S. vendors are not eligible to ship encryption products to 403 of the so-called Global 1000 multinational corporations named by *Fortune* magazine. Because many foreign-based procurements include security in the specification for the total procurement, U.S. firms often lose out to foreign firms (e.g., in the United Kingdom or Switzerland) that do not face the same restrictions ( ibid. ).

origin products containing encryption implemented in hardware, soft ware, and hardware/software combinations. According to SPA, 245 of these products use the DES and, therefore, are subject to ITAR controls and cannot be exported except in very limited circumstances. [146] In total, SPA identified 763 cryptographic products, developed or distributed by a total of 366 companies (211 foreign, 155 domestic) in at least 33 countries. '[47] In addition, software implementations of the DES and other encryption algorithms are routinely available on Internet sites worldwide. '48

At the hearing, Walker showed examples of DES-based products that SPA had taken delivery on from vendors in Denmark, the United Kingdom, Germany, and Russia. Walker also demonstrated how laptop computers (with internal speakers and microphones) could be transformed into encrypting telephones, using a DES-based software program purchased in the United States to encrypt/decrypt digital speech.[149]

Based on experiences like this, many in industry consider that the foreign-dissemination control objectives of the current export regime serve mainly to hinder domestic firms that either seek to sell or use cryptography:

> Foreign customers who need data security now turn to foreign rather than U.S. sources to fulfill that need. As a result, the U.S. government is succeeding only in crippling a vital American industry's exporting ability. [150]

The impact of export controls on the overall cost and availability of safeguards is especially troublesome to business and industry at a time when U.S. high-technology firms find themselves as targets for sophisticated foreign-intelligence attacks [151] and thus have urgent need for sophisticated safeguards that can be used in operations worldwide. 152 Moreover, software producers assert that several other countries do have more relaxed export controls on cryptography:

> Our experience. . . has demonstrated conclusively that U.S. business is at a severe disadvantage in attempting to sell products to the world market. If our competitors overseas can routinely ship to most places in the world within days and we must go through time-consuming and onerous procedures with the most likely outcome being denial of the export request, we might as well not even try. And that is exactly what many U.S. companies have decided.

---

146 Walker testimony, op. cit., footnote 37, p. 15.

147 Ibid.

148 Software Publishers Association, "SPA Study of Foreign Availability of Cryptographic Products, " updated Jan. 1, 1994, and Walker testimony, op. cit., footnote 37. In one case, the author of PGP (Pretty Good Privacy), a public-key encryption software package for email protection, was investigated by the U.S. Customs Service. In April 1994, a federal grand jury was examining whether the author broke laws against exporting encryption software. POP was published in the United States as "freeware" in June 1991 and has since spread throughout the world via networks, RSA Data Security, Inc. says that the POP versions available via the Internet violate the RSA patent in the United States. (See William M. Bulkeley, "Popularity Overseas of Encryption Code Has the U.S. Worried," *The Wall Street Journal*, Apr. 28, 1994, pp. 1, A8; and John Markoff, "Federal Inquiry on Software Examines Privacy Programs," *The New York Times*, Sept. 21, 1993, pp. D1, D7.).

149 Walker testimony, op. cit., footnote 37, pp. 14-20 and attachment. According to Walker, SPA had also received encryption products from Australia, Finland, and Israel.

150 Walker testimony, 0p. cit., footnote 37, pp. 15-26 (quote at 15). See also SPA and BSA, op. cit., footnotes 148 and 136.

151 Th, Threat *of Foreign Economic Espionage to U.S. Corporations*, hearings, op. *cit.*, footnote 2.

152 See GAO, op. Cit., footnote 4.8, p. 4 (citing the Director, Central Intelligence Agency); and U.S. General Accounting Office, *Economic Espionage: The Threat to U.S. Industry*, GAO/OSI-92-6 (Washington, DC: U.S. Government Printing Office, 1992). (Statement of Milton J. Socolar, testimony before the Subcommittee on Economic and Commercial Law, Committee on the Judiciary, U.S. House of Representatives, Apr. 29, 1992.)

> And please be certain to understand that we are not talking about a few isolated products involving encryption. More and more we are talking about major information processing applications like word processors, databases, electronic mail packages, and integrated software systems that must usc cryptography to provide even the most basic level of security being demanded by multinational companies.[153]

On the other hand, U.S. export controls may have substantially slowed the proliferation of cryptography to foreign adversaries over the years. Unfortunately, there is little explanation (at least at the unclassified level) regarding the degree of success of these export controls and the necessity for maintaining strict controls on strong cryptography in the face of foreign supply and networks like the Internet that seamlessly cross national boundaries. (For a general discussion of the costs and benefits of export controls on dual-use goods see OTA's recent report *Export Controls and Nonproliferation Policy, OTA-ISS-596,* May 1 994.)

Some of the most recent public justifications for continued strict controls were made in May 1994 testimonies by Vice Admiral J.M. McConnell (NSA Director) and Clinton Brooks (Special Assistant to the Director, NSA):

> Clearly, the success of NSA's intelligence mission depends on our continued ability to collect and understand foreign communications ... Controls on encryption exports arc important to maintaining our capabilities.
>
> ... At the direction of the President in April, 1993, the Administration spent ten months carefully reviewing its encryption policies, with particular attention to those issues related to export controls on encryption products. The Administration consulted with many industry and private sector representatives and sought their opinions and suggestions on the entire encryption export control policy and process. As a result of this review, the Administration concluded that the current encryption export controls are in the best interest of the nation and must be maintained, but that some changes should be made to the export licensing process in order to maximize the exportability of encryption products and to reduce the regulatory burden on exporters. These changes will greatly case the licensing process and allow exporters to more rapidly and easily export their products.
>
> In addition, the Administration agreed at the urging of industry that key escrow encryption products would be exportable. Our announcement regarding the exportability of key escrow encryption products has caused some to assert that the Administration is permitting the export of key escrow products while controlling competing products in order to force manufacturers to adopt key escrow technology. These arguments arc without foundation. . .we are not using or intending to use export controls to force vendors to adopt key escrow technology. ] 54

Clinton Brooks also noted that:

> The U. S., with its key escrow concept, is presently the only country proposing a technique that provides its citizens very good privacy protection while maintaining the current ability of law enforcement agencies to conduct lawful electronic surveillance. Other countries arc using government licensing or other means to restrict the usc of encryption.[155]

In February 1994, the Clinton Administration announced its intention to reform the export control procedures that apply to products incorporating encryption technology:

> These reforms are part of the Administration's effort to eliminate unnecessary controls and ensure efficient implementation. The reforms will simplify encryption product export

[153] Walker testimony, op. cit., footnote 37, p. 18.

[154] McConnell testimony, op. cit., footnote 8, p. 6; and Clinton C. Brooks, Special Assistant to the Director, NSA, testimony before the Subcommittee on Technology, Environment and Aviation, Committee on Science, Space, and Technology, U.S. House of Representatives, May 3, 1994, pp. 5-6. (Identical passage in both.)

[155] Clinton Brooks testimony, ibid., p. 4. (Similar statement in McConnell, ibid., pp. 3-4.)

> licensing and speed the review of encryption product exports, thus helping U.S. manufacturers to compete more effectively in the global market. While there will be no changes in the types of equipment controlled by the Munitions List, we are announcing measures to expedite licensing. [156]

The new licensing procedures were expected to appear in the *Federal Register* in June 1994.[157] According to the State Department, the reforms "should have the effect of minimizing the impact of export controls on U.S. industry. ''158 These were expected to include:

- license reform measures that will enable manufacturers to ship their products directly to customers within approved regions, without obtaining individual licenses for each end user;
- rapid review of export license applications (a "significant" number of applications will have a turnaround goal of 10 working days);
- personal use exemptions for U.S. citizens temporarily taking encryption products abroad for their own use (previously, an export license was required); and
- allowing exports of key-escrow encryption products to most end users (key-escrow products will qualify for special licensing arrangements). [159]

The Secretary of State has asked encryption product manufacturers to evaluate the impact of these reforms over the next year and provide feedback on how well they have worked, as well as recommendations for additional procedural reforms. [160]

In the 103d Congress, legislation intended to streamline export controls and ease restrictions on mass-market computer software, hardware, and technology, including certain encryption software, was introduced by Representative Maria Cantwell (H.R. 3627) and Senator Patty Murray (S. 1846). In considering the Omnibus Export Administration Act (H.R. 3937), the Committee on Foreign Affairs reported a version of the bill in which most computer software, including software with encryption capabilities, was under Commerce Department controls and in which export restrictions for mass-market software with encryption were eased.[161] The Report of the Permanent Select Committee on Intelligence struck out this portion of the bill and replaced it with a new section calling for the President to report to Congress within 150days of enactment, regarding the current and future international market for software with encryption and the economic impact of U.S. export controls on the U.S. computer software industry. [162]

At this writing, the omnibus export administration legislation was still pending. Both the House and Senate bills contained language calling for the Administration to conduct comprehensive studies on the international market and availability of encryption technologies and the economic effects of U.S. export controls.

## SAFEGUARDS, STANDARDS, AND THE ROLES OF NIST AND NSA

This section summarizes current NIST and NSA activities related to safeguards for unclassified information, as well as joint activities by the two

---

156 Martha Harris, op. cit., footnote 129.

157 Rose Biancaniello, Office of Defense Trade Controls, Bureau of Political-Military Affairs, U.S. Department of State, personal communication, May 24, 1994.

158 Martha Harris, op. cit., footnote 129.

159 Ibid.

160 Ibid.

161 See *Omnibus Export Administration Act of 1994*, op. cit., footnote 116, Part 1, pp. 57-58 (H.R. 3937, sec. 117(c)(1)-(4)).

162 *Omnibus Export Administration Act of 1994*, op. cit., footnote 116, Part 2, pp. 1-5 (H.R. 3937, sec. 117(c)(1)-(3)).

agencies. It also discusses the current, controversial interagency agreement describing the agencies' implementation of the Computer Security Act.

## NIST Activities in Support of Information Security and Privacy

Ongoing NIST activities in support of information security and privacy in the High Performance Computing and Communications/National Information Infrastructure (HPCC/NII) Programs are conducted by NIST's Computer Systems Laboratory.[163] The overall objectives of the HPCC/NII Programs are to accelerate the development and deployment of high-performance computing and net working technologies required for the NII; to apply and test these technologies in a manufacturing environment; and to serve as coordinating agency for the manufacturing component of the federal HPCC Program. NIST contributes to the following components of the federal HPCC Program:

- high performance computing systems,
- advanced software technology and algorithms,
- National Research and Education Network, and
- information infrastructure technology and applications[164]

According to NIST's interpretation of policy guidance received from OMB, no agency has the lead with respect to security and privacy in support of the NH; accordingly, NIST and other agencies support OMB initiatives.[165] NIST's summary of NII-related security projects is reproduced in box 4-7.

NIST has also announced two opportunities to join cooperative research consortia in support of key-escrow encryption. In August 1993, NIST announced an ● 'Opportunity to Join a Cooperative Research and Development Consortium to Develop Software Encryption with Integrated Cryptographic Key Escrowing Techniques." According to the announcement, this research would be done in furtherance of the key-escrowing initiative announced by President Clinton on April 16,

[163] As this report was written, NIST was in the process of reorganizing to create a new Information Technology Laboratory; [he CSL activities are expected to be included in the functions of the Information Technology Laboratory. See also Dennis M. Gilbert, *A Study of Federal Agency Needs for in/orma(Ion Technology Security*, NISTIR-5424 (Gaithersburg, MD: NIST, May 1994) for the results of a NIST study to be used for planning future NI ST In formation technology security standards, guidance, and related activities.

[164] "Proposed HPCC NII Program at NIST," May 1993. Included in attachment 2 of a letter from F. Lynn McNulty, Associate Director for Computer Security, NIST, to Joan D. Winston, OTA, Apr. 13, 1994. OTA had requested information about current NIST activities in support of the information Infrastructure and about security/privacy related information in letters to NIST dated Feb. 28, 1994 and Mar. 11, 1994.

[165] F.L McNulty, ibid. See also Gilbert, op. cit., footnote 163.

## BOX 4-7: NIST Computer Security Division

*The Office of Technology Assessment asked the National Institute of Standards and Technology for a summary of activities related to computer and information security The information provided by NIST in April 1994 is reproduced below:*

Issue Area: **Information Security**

**Objective** *Areas: All*

Information security is an important issue in all the objective areas. In addition, information security is a cross-cutting issue for three other areas: privacy, protecting intellectual property, and controlling access to information since the ability to ensure privacy, protection of intellectual property, and controlled access to information will require that information security controls are in place and operating correctly.

*Project:* **Digital Signature Standard and Supporting Infrastructure**

This project provides the technology to electronically sign multi-media information, to ensure non-repudiation of the originator and receiver of the information, and to detect modifications to the information It also focuses on establishing the supporting infrastructure needed to distribute certificates to users in government and commercial interactions. Certificates are necessary since they contain unforgeable information about the identity of the individual presenting the certificate and contain other components required for the digital signature function.

*Project:* **Cryptographic Standards**

This project area includes basic cryptographic-based standards that are needed throughout the [National Information Infrastructure] Nll "electronic highway" and within applications in most, if not all objective areas. In addition, it includes a standard (metric) for the level of security of cryptographic mechanisms used throughout the Nll.

*Project:* **Advanced Authentication Technology**

The vast majority of current [information technology] IT systems continue to rely on passwords as the primary means of authenticating legitimate users of such systems Unfortunately, vulnerabilities associated with the use of passwords have resulted in numerous intrusions, disruptions, and other unauthorized activity to both government and commercial IT systems. NIST activities in this area have focused on moving federal agencies away from reliance on passwords to the use of token based and other technologies for authenticating users. Specifically, the [Computer Security Division] CSD has been working directly with federal agencies to incorporate advanced authentication technology (as well as other security technologies) into their applications to provide better cost effective security Such applications are/will be included as components of the Nll (e g , IRS tax filing applications).

*Project:* **Security Criteria and Evaluation**

The goal of this project area is to develop an internationally accepted security which can be used to specify the security functionality and assurance requirements of IT systems and products and to establish a U.S. government capability to verity that the developer of the product/system has met both sets of requirements. The long term goal of this project is a plentiful supply of secure commercial off-the-shelf products that will be used in Nll applications and other part of the Nil.

*Project:* **Secure the Internet and Network Connectivity**

This project focuses on providing near term assistance and solutions for organizations that must connect to the Internet and other networks.

*(continued)*

## BOX 4-7 (cont'd.): NIST Computer Security Division

*Project:* **Open Systems Security**

This project area focuses on longer term activities that will result in enhanced security for government applications on the Nll. These include the extension of security labels to other IT areas and extensions of the DOD Goal Security Architecture to other government systems Security labels are necessary for specifying the type and sensitivity of information stored m a host system or being communicated from one party to another

*Project:* **Computer Security Management**

The best technical solutions will not be effective unless there is a managed combination of technology Pollees procedures and people All applications within the Nll will require security management if they are to provide cost effective security to users of the Nll. This project focus on management activities such as traming/education, risk management, and accepted security practices that ensure use of security technology

SOURCE National Institute of Standards and Technology, April 1994

1993.[166] A February 1994 NIST press release[167] announced partnership opportunities in research directed at developing computer hardware with integrated cryptographic key-escrowing techniques. [168] The cooperative research involves technical assistance from NSA. As of June 1994, NIST reported that several individuals and organizations were participating in a Key Escrow Encryption Working Group seeking to "specify requirements and acceptability criteria for key-escrow encryption systems and then design and/or evaluate candidate systems.''[169]

In early 1994, OTA asked the National Institute of Standards and Technology for more information on the resources that would be required—staff, funds, equipment, and facilities—to set up NIST as a key-escrow agent. NIST had originally estimated that startup costs for both escrowing facilities would be about $14 million, with total annual operating costs of about $16 million. [170] In April 1994, NIST told OTA that the Clinton Administration was still working on cost estimates for the escrow system and was not able to release additional cost information.[171] By June 1994, 17,000 Clipper chip keys had been escrowed at NIST.[172] OTA has not received any additional information regarding costs, staffing, and other resource requirements for the escrow system.

Funding for NIST's computer-security activities is shown in table 4-1. According to the figures in table 4-1, appropriated funds for computer security show an almost fourfold increase from levels prior to the Computer Security Act of 1987. This does not represent steady growth, however; there was a large increase from $1.0 million in FY

166 *Federal Register, Aug. 24,* 1993, pp. 44662-63. (This announcement was written before the EES was finalized. )

167 "NIST Calls for Partners in Developing Key Escrowing Hardware," Feb. 4, 1994. (The EES was finalized. )

168 This materialwasattachment of McNulty, Apr. 13, 1994, op. cit., footnote 164.

169 Miles Smid, NIST, "The U.S. Government Key Escrow System," presentation at NIST Key Escrow Encryption Workshop, June 10, 1993. These activities support the Administration's exploration of alternative key-escrow encryption techniques, as announced in a July 20, 1994, letter from Vice President Al Gore to Representative Maria Cantwell.

170 *Federal Register*, Feb. 9, 1994, p. 6000.

171 I F. Lynn McNulty, NIST Associate Director for Computer Security, letter to Joan Dopico Winston, OTA, Apr. 13, 1994.

172 Miles Smid Manager, Security Technology Group, N] ST, personal communication, May 25, 1994.

TABLE 4-1: Computer Security ($ millions)

| Fiscal year | Obligations: Appropriation funds | Obligations: Reimbursable | Full-time equivalents |
|---|---|---|---|
| 1985 | 12 | 05 | 16 |
| 1986 | 1.1 | 0.4 | 16 |
| 1987 | 1.1 | 04 | 16 |
| 1988 | 1,0 | 0.7 | 17 |
| 1989 | 2.7 | 0.8 | 33 |
| 1990 | 2,7 | 0 8 | 33 |
| 1991 | 3.3 | 1.6 | 37 |
| 1992 | 3 4 | 2.3 | 35 |
| 1993 | 3.9 | 2.1 | 35 |
| 1994 | *4.4* | 2.0 | 38 est. |
| 1995 | 4.5 | 20 | 38 est. |

"The enactment of the Computer Security Act in 1988 imposed new responsibilities on the National Institute of Standards and Technology to improve the security and privacy of sensitive information in computer systems of all federal agencies. In addition to responsibilities for developing standards and guidelines and for carrying out research in computer security, NIST was assigned the responsibility for reviewing agency computer security plans, assisting in the development of training programs agencies, and establishing and operating a Computer System Security and Privacy Advisory Board. NIST used appropriated funds to hire a core staff to carry out the general tasks assigned by the law. Reimbursable funds were used for tasks that were specific to the other agencies. Additional reimbursable tasks have been accepted to respond to increased demands for help as agency awareness of their computer security responsibilities has increased. These reimbursable tasks have been accepted only when they support the goals of NIST's Computer Security Program."

SOURCE: National Institute of Standards and Technology, April 1994.

1988 to $2.7 million in FY 1989 and FY 1990, and slower growth thereafter. Staffing levels also rose, from 17 full-time equivalents (FTEs) in FY 1988 to an average of 36 or 37 FTEs thereafter. Since 1990, "reimbursable" funds received from other agencies (mainly DOD) have been substantial compared with appropriated funds for security-related activities, representing some 30 to 40 percent of the **total** funding for computer-security activities and staff at CSL. This is a large fraction of what has been a relatively small budget, given NIST's responsibilities under the Computer Security Act.

## Joint NIST/NSA Activities

**In** January 1994, OTA asked NSA for a summary of the activities NSA reported that it conducted jointly with NIST under the Computer Security Act of 1987. According to NSA, these include the National Computer Security Conference, development of common criteria for computer security (see chapter 2), product evaluations, standards development, and research and development. OTA received this information in April 1994; it is reproduced in box 4-8.

## NIST/NSA Implementation of the Computer Security Act of 1987

A 1989 Memorandum of Understanding between the NIST Director and the NSA Director established the mechanisms of the working relationship between NIST and NSA in implementing the Computer Security Act of 1987.173 The MOU has been controversial. Observers-including OTA —consider that the MOU appears to cede to NSA much more authority than the act itself had granted or envisioned, particularly through the joint NIST/NSA Technical Working Group established by the MOU.[174] In May 1989, Milton J. Socolar, Special Assistant to the Comptroller General, noted:

> . . . as one reviews the [MOU] itself against the background of the [Computer Security A]ct, one cannot help but be struck by the extent of influence NSA appears to retain over the processes

1 73 *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,* Mar. 23,1989. (See appendix B.)

174 The Technical Working Group may identify issues for discussion, or these may be referred to it by the NSA Deputy Director for Information Security or the NIST Deputy Director (ibid., sec. 111(5)).

## BOX 4-8: Overview of Joint NIST/NSA Activities

*The Office of Technology Assessment asked* NSA *for a summary of joint NIST-NSA activities, The material provided by NSA in April 1994 is reproduced below:*

NSA provides technical advice and assistance to NIST in accordance with Public Law 100-235 An overview of NIST-NSA activities follows

National Conference. NIST and NSA jointly sponsor, organize, and chair the prestigious National Computer Security Conference, held yearly for the past 16 years The conference IS attended by over 2,000 people from government and private Industry

**Common Criteria** NSA is providing technical assistance to NIST for the development of computer security criteria that would be used by both the civilian and defense sides of the government Representatives from Canada and Europe are joining the United States in the criteria's development

**Product Evaluations.** NIST and NSA are working together to perform evaluations of computer security products In the Trusted Technology Assessment Program, evaluations of some computer security products will be performed by NIST and their labs, while others will be performed by NSA. NIST and NSA engineers routinely exchange Information and experiences to ensure uniformity of evaluations

**Standards Development.** NSA supports NIST **in** the development of standards that promote interpretability among security products Sample standards include security protocol standards, digital signature standards, key management standards, and encryption algorithm standards (e g , the DES, SKIPJACK)

**Research and Development** Under the Joint R&D Technology Exchange Program, NIST and NSA hold periodic technical exchanges to share Information on new and ongoing programs Research and development IS performed in areas such as security architectures, labeling standards, privilege management, and identification and authentication Test-bed activities are conducted in areas related to electronic mail, certificate exchange/management, protocol conformity, and encryption technologies

SOURCE National Security Agency, April 1994

involved in certain areas-an influence the act was designed to diminish. [175]

In response to concerns and questions raised in the May 1989 hearings, NIST and NSA prepared a letter of clarification for the House Committee on Government Operations. This December 22, 1989, letter was intended to assuage concerns.[176] However, concerns that neither the MOU or the letter of clarification accurately reflected the intent of the Computer Security Act continued. '77 A February 1990 letter to the committee from the Secretary of Commerce and subsequent staff dis-

175 Milton J. Socolar, Special Assistant to the Comptroller General, "National Institute of Standards and Technology and the National Security Agency's Memorandum of Understanding on Implementing the Computer Security Act of 1987," in *Hearing on Military and Civilian Control of Compiler Security Issues,* May *4, 1989,* op. cit., footnote 99, pp. 39-47, quote at p. 47. Socolar also noted other concerns, such as the MOU appeal process in sec. III(7), the NSA evaluation of security programs, NSA research and development activities, NIST recognition of NSA-certified ratings of trusted systems, and other matters.

176 Letter to Rep. John Conyers, Jr., and Rep. Frank Horton from Raymond Kammer (NIST) and W. O. Studemann (NSA), Dec. 22, 1989. (See appendix B.)

177 See Richard A. Danca and Robert Smithmidford, "NSA, NIST Caught in Security Policy Debate," *Federal Computer Week, Feb.* 12, 1990, p. 1,

cussions continued to explore these concerns. '78 (See appendix B of this report for the MOU, the December 1989 NIST/NSA letter of clarification, and the February 1990 letter from the Secretary of Commerce.)

Implementation of the Computer Security Act remains controversial; the MOU has not—to the best of OTA's knowledge—been modified. A recent GAO study found that:

> The Computer Security Act of 1987 reaffirmed NIST as the responsible federal agency for developing federal cryptographic information-processing standards for the security of sensitive, unclassified information. However, NIST has followed NSA's lead when developing certain cryptographic standards for communications privacy. [179]

The MOU authorizes NIST and NSA to establish a Technical Working Group (TWG) to "review and analyze issues of mutual interest pertinent to protection of systems that process sensitive or other unclassified information." The TWG has six members; these are federal employees, with three selected by NIST and three selected by NSA. The working group membership may be augmented as necessary by representatives of other federal agencies.

Where the act had envisioned NIST calling on NSA's expertise at its discretion, the MOU's TWG mechanism involves NSA in all NIST activities related to information-security standards and technical guidelines, as well as proposed research programs that would support them. The implementation mechanisms defined by the MOU include mandatory review by the TWG, prior to public disclosure, of "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." 180 If NIST and NSA cannot resolve such an issue within 60 days, either agency can elect to raise it to the Secretary of Defense and Secretary of Commerce, or to the President through the National Security Council. No action can be taken on an issue until it is resolved. Thus, the MOU provisions give NSA power to delay and/or appeal any NIST research programs involving "technical system security techniques" (such as encryption), or other technical activities that would support (or could lead to) proposed standards or guidelines that NSA would ultimately object to. [181]

NSA reviewers who commented on a draft of this OTA report disagreed with this interpretation. According to these reviewers, the Computer Security Act did not take into account that the techniques NIST would consider in developing standards for information systems that process unclassified information:

> . . . have the potential to thwart law enforcement and national intelligence activities. NIST recognized that they needed a mechanism to obtain NSA's expertise and to understand the risk that certain security techniques could pose for these activities. Moreover, they needed to understand these risks before the proposed standards were promulgated and the damage was done. The MOU between NIST and NSA provided this mechanism. Rather than delay NIST standards, the MOU process provides NIST critical information it needs in formulating the standards. [182]

In subsequent discussions with OTA staff, NSA officials reiterated this point and explained that

---

178 Letter to Chairman John Conyers, Committee on Government Operations, from Robert A. Mosbacher, Secretary of Commerce, Feb. 28, 1990. An enclosure t. this letter elaborates on matters raised by the committee staff in a meeting on Jan. 3, 1990. (The MOU and both the December 1989 and February 1990 letters are found in appendix B of this report.)

179 GAO, Op. cit., footnote 48, p. 5, using the DSS as evidence.

180 MOU, op. cit., footnote 173, sec. 111(7).

181 ibid., sees. 111(5)-(7). See also M.J. Socolar, op. Cit., footnote 175, pp. 45-46.

182 Roger M Callahan, NSA, letter to Joan D. Winston, OTA, May 6, 1994, p. 4.

the appeals process specified in the Computer Security Act (see below) would come too late in the standards process to avoid harming national-security and law-enforcement interests.[183]

NIST's most recent efforts to develop a public-key standard and a digital signature standard have focused concerns on the MOU and the working relationship between NIST and NSA. NIST standards activities related to public-key cryptography and digital signatures have proceeded intermittently for over 12 years. Much of the original delay (i.e., 1982-89) appears to have been due to national-security, nonproliferation concerns voiced by NSA.[184] (The most recent delay resulted from patent-licensing problems—see appendix C.)

NBS (now, NIST) originally published a "Solicitation for Public Key Cryptographic Algorithms" in the *Federal Register* on June 30, 1982. According to the results of a classified investigation by GAO, NBS abandoned this standards activity at the request of NSA.[185] In 1989, after the Computer Security Act, NIST again began discussions with NSA about promulgating a public-key standard that could be used for signatures. These discussions were conducted through the Technical Working Group mechanism established in the MOU, which had been signed earlier that year. According to GAO, at the start of these discussions, the NIST members of the Technical Working Group had preferred the RSA algorithm because it could be used for signatures and also could encrypt for confidentiality (and, therefore, be used for cryptographic key management/exchange).[186] According to GAO, the plan to select a public-key algorithm that could do both signatures and key exchange was terminated in favor of a technique, developed under NSA funding, that only did signatures.[187] Another motive for selecting a different algorithm was that the RSA method was patented, and NIST wanted to develop a royalty-free standard.

NSA's algorithm is the basis for the DSS. It performs the signature function but does not encrypt for purposes of confidentiality or secure key distribution. The Capstone and TESSERA implementations of the EES encryption algorithm also include digital signature and key-exchange algorithms, but as of June 1994 this key-exchange algorithm was not part of a FIPS.

As originally proposed in 1991, the DSS met with several types of criticism. Some criticisms were on technical grounds, including the strength of the algorithm. In response, NIST and NSA revised the proposed standard, increasing the maximum size of the modulus from 512 to 1,024

183 Clinton Brooks, Special Assistant to the Director, NSA, personal communication, May 25, 1994.

184 Public-key cryptography can be *used* for data encryption, digital signatures, and in cryptographic key management/exchange (to securel y distribute secret keys). Current federal standards initiatives take the approach of devising ways to do signatures (i.e., the DSS) and key distribution without also providing data encryption capabilities.

185 GAO, OP. cit., footnote 48, p. 20.

186 ibid. GAO based this conclusion on NIST memoranda.

187 Ibid pp. 20.21. GAO based [his conclusion on NIST memoranda. See also the series of NIST/NSA Technical Working Group minutes from May 1989 to August 1991, published in "Selected NIST/NSA Documents Concerning the Development of the Digital Signature Standard Released in *Computer Professionals for Social Responsibility v. National Institute of Standards and Technology, Civil* Action No. 92-0972," Computer Professionals for Social Responsibility, *The Third Cryptography and Privacy Conference Source Book*, June 1993. (Note: According to NSA, the materials obtained through the Freedom of Information Act are not a true picture of all the different levels of discussion that took place during this period, when NIST management and NSA were in agreement regarding the development of a signature standard. Clinton Brooks. Special Assistant to the Director, NSA, personal communication, May 25, 1994.)

See also D.K. Branstad and M.E. Smid, "Integrity and Security Standards Based on Cryptography," *Computers & Security*, vol. *I ( 1982)*, pp. *255-2@;* Richard A. Danca, "Torricelli Charges NIST with Foot-Dragging on Security," *Federal Computer Week*, Oct. 8, 1990, p. 9; and Michael Alexander, "Data Security Plan Bashed," *Computerworld*, July 1, 1991, p. 1

bits.[188] (Increasing the number of bits in the modulus increases strength, analogous to increasing the length of a key.) Other criticisms focused on possible patent infringement and licensing issues (see appendix C). The DSS was finished and issued by the Commerce Department in May 1994, to take effect on December 1, 1994, with the statements that:

> NIST has addressed the possible patent infringement claims, and has concluded that there are no valid claims. [189]
>
> The Department of Commerce is not aware of any patents that would be infringed by this standard.[190]

As this report went to press, the possibility of infringement litigation was still open (see appendix C).

The Computer Security Act envisioned a different standards-appeal mechanism. According to the act, the President could disapprove or modify standards or guidelines developed by NIST and promulgated by the Secretary of Commerce, if he or she determined such an action to be in the public interest. The President cannot delegate authority to disapprove or modify proposed NIST standards.[191] Should the President disapprove or modify a standard or guideline that he or she determines will not serve the public interest, notice of such action must be submitted to the House Committee on Government Operations and the Senate Committee on Governmental Affairs, and must be published promptly in the *Federal Register*.[192] By contrast, interagency discussions and negotiations by agency staffs under the MOU can result in delay, modification, or abandonment of proposed NIST standards activities, without notice or the benefit of oversight that is required by law.

NIST and NSA disagree with this conclusion. According to NIST and NSA officials, NIST has retained its full authority in issuing the FIPS and NSA's role is merely advisory. In May 1994 testimony before the House and Senate, the NIST Deputy Director stated that:

> The Act, as you are aware, authorizes NIST to draw upon computer security guidelines developed by NSA to the extent that NIST determines they are consistent with the requirements for protecting sensitive information in federal computer systems. In the area of cryptography, we believe that federal agencies have valid requirements for access to strong encryption (and other cryptographic-related standards) for the protection of their information. We were also aware of other requirements of the law enforcement and national security community. Since NSA is considered to have the world's foremost cryptographic capabilities, it only makes sense (from both a technological and economic point of view) to draw upon their guidelines and skills as useful inputs to the development of standards. The use of NSA-designed and -tested algorithms is fully consistent with the Act. We also work Jointly with NSA in many other areas, including the development of criteria for the security evaluation of computer systems. They have had more experience than anyone else in such evaluations. As in the case of cryptography, this is an area in which NIST can benefit from NSA's expertise. [193]

According to the NSA Director:

> Our role in support of [the Clinton Administration's key escrow initiative] can be summed

188 "Digital signature Standard (DSS)—Draft," FIPS PUB XX, National Institute of Standards and Technology, Feb. 1, 1993.

189 *Federal Register*, May 19, 1994, op. cit., footnote 16, p. 26209.

190 ibid., p. 26210; also NIST, op. cit., footnote 26, p. 3.

191 Computer Security Act of 1987, sec. 4.

192 Ibid.

193 Kammer testimony, May 3, 1994, op. Cit., footnote 13, pp. 12-13. (The same written testimony was presented to the subcommittee on Technology and Law, Committee on the Judiciary, U.S. Senate, in the morning and to the Subcommittee on Technology, Environment and Aviation, Committee on Science, Space, and Technology, U.S. House of Representatives, in the afternoon.)

up as "technical advisors" to [NIST] and the FBI.

As the nation's signals intelligence (SIGINT) authority and cryptographic experts, NSA has long had a role to advise other government organizations on issues that relate to the conduct of electronic surveillance or matters affecting the security of communications systems. Our function in the latter category became more active with the passage of the Computer Security Act of 1987. The act states that the National Bureau of Standards (now NIST) may, where appropriate, draw upon the technical advice and assistance of NSA. It also provides that NIST must draw upon computer system technical security guidelines developed by NSA to the extent that NIST determines that such guidelines are consistent with the requirements for protecting sensitive information in federal computer systems. These statutory guidelines have formed the basis for NSA's involvement with the key escrow program.

Subsequent to the passage of the Computer Security Act, NIST and NSA formally executed a memorandum of understanding (MOU) that created a Technical Working Group to facilitate our interactions. The FBI, though not a signatory to the MOU, was a frequent participant in our meetings. . . In the ensuing discussions, the FBI and NIST sought our technical advice and expertise in cryptography to develop a technical means to allow for the proliferation of top quality encryption technology while affording law enforcement the capability to access encrypted communications under lawfully authorized conditions. [194]

In discussions with OTA, officials from both agencies maintained that no part of the MOU is contrary to the Computer Security Act of 1987, and that the controversy and concerns are due to misperceptions. [195] When OTA inquired about the MOU/TWG appeals process in particular, officials in both agencies maintained that it does not conflict with the Computer Security Act of 1987 because the MOU process concerns *proposed* research and development projects that could lead to *future* NIST standards, not *fully-developed* NIST standards submitted to the Secretary of Commerce or the President. [196] GAO has previously noted that NIST considered the process appropriate because:

> . . . NSA presented compelling national security concerns which warranted early review and discussion of NIST's planned computer security related research and development. If concerns arise, NSA wanted a mechanism to resolve problems before projects were initiated. [197]

In discussions with OTA, senior NIST and NSA staff stated that the appeals mechanism specified in the Computer Security Act has never been used, and pointed to this as evidence of how well the NIST/NSA relationship is working in implementing the act. [198] These agency officials also told OTA that the working interactions between the agency staffs have improved over the past few years. In discussions with OTA staff regarding a draft of this OTA report, Clinton Brooks, Special Assistant to the Director of NSA, stated that cryptography presents special problems with respect to the Computer Security Act, and that if NSA waited until NIST announced a proposed standard to voice national security concerns, the technology would already be "out" via NIST's public standards process. [199]

However, even if implementation of the Computer Security Act of 1987, as specified in the

194 McConnell testimony, op. cit., footnote 8, pp. 1-2. Similar passage in Clinton Brooks testimony, op. cit., footnote 154, pp. 1-2.

195 OTA staff interviews with NIST and NSA officials in October 1993 and January 1994. See also Socolar, op. cit., footnote 153, p. 45.

196 OTA staff interviews, ibid.

197 Socolar, op. cit., footnote 153, p. 45.

198 OTA staff interview with M. Rubin (Deputy Chief Counsel, NIST) on Jan. 13, 1994 and with four NSA staff on Jan. 19, 1994.

199 Clinton Brooks, Special Assistant to the Director, NSA, personal communication, May 25, 1994.

MOU, is satisfactory to both NIST and NSA, this is not proof that it meets Congress' expectations in enacting that legislation. Moreover, chronic public suspicions of and concerns with federal safeguard standards and processes are counterproductive to federal leadership in promoting responsible use of safeguards and to public confidence in government.

With respect to the EES, many public concerns stem from the secrecy of the underlying SKIPJACK algorithm, and from the closed processes by which the the EES was promulgated and is being deployed. Some of these secrecy-related concerns on the part of industry and the public have focused on the quality of the algorithm and hesitation to use federal endorsement alone (rather than consensus and widespread inspection) as a quality guarantee.[200] Others have focused on another consequence of the use of a classified algorithm—the need to make it only available in tamper-resistant modules, rather than in software. Still other concerns related to secrecy focus on a situation where:

> ... authority over the secret technology underlying the standard [FIPS 185] and the documents embodying this technology, continues to reside with NSA. We thus have a curious arrangement in which a Department of Commerce standard seems to be under the effective control of a Department of Defense agency. This appears to violate at least the spirit of the Computer Security Act and strain beyond credibility its provisions for NIST's making use of NSA's expertise.[201]

To remedy this, Whitfield Diffie, among others, has suggested that:

> Congress should press the National Institute of Standards and Technology, with the cooperation of the National Security Agency, to declassify the SKIPJACK algorithm and issue a revised version of FIPS 185 that specifies the algorithm and omits the key escrow provisions. This would be a proper replacement for FIPS 46, the Data Encryption Standard, and would serve the needs of the U.S. Government, U.S. industry, and U.S. citizens for years to come.[202]

It may be the case that using two executive branch agencies as the means to effect a satisfactory balance between national security and other public interests in setting safeguard standards will inevitably be limited, due to intrabranch coordination mechanisms in the National Security Council and other bodies. These natural coordination mechanisms will determine the balance between national-security interests, law-enforcement interests, and other aspects of the public interest. The process by which the executive branch chooses this balancing point may inevitably be obscure outside the executive branch. (For example, the Clinton Administration's recent cryptography policy study is classified, with no public summary.) Public "visibility" of the decision process is through its manifestations—in a FIPS, in export policies and procedures, and so forth. When the consequences of these decisions are viewed by some (or many) of the public as not meeting important needs, or when the government's preferred technical "solution" is not considered useful, a lack of visibility, variety, and/or credible explanation fosters mistrust and frustration.

Technological variety is important in meeting the needs of a diversity of individuals and communities. Sometimes federal safeguard standards are eventually embraced as having broad applicability. But it is not clear that the government can-or

---

200 A more open inspection process prior to issuance of the EES would have allowed issues like the possible protocol failures in implementing the law-enforcement access field to be dealt with before they became sensationalized in the press, See John Markoff, "Flaw Discovered in Federal Plan for Wiretapping," *The* New *York Times*, June 2, 1994, p. I and p. D 17; and "At AT&T, No Joy in Clipper Flaw," *The New York Times*, June 3, 1994, pp. D1,D2.

201 Diffie testimony, op. cit., footnote 24, p. 6.

202 Ibid., pp. IO-1 1.

should--develop all-purpose technical safeguard standards, or that the safeguard technologies being issued as the FIPS can be made to meet the full spectrum of user needs. More open processes for determining how safeguard technologies are to be developed and/or deployed throughout society can better ensure that a variety of user needs are met equitably.

If it is in the public interest to provide a wider range of technical choices than those provided by government-certified technologies (i.e., the FIPS), then vigorous academic and private-sector capabilities in safeguard technologies are required. For example, private users and corporations might want the option of using third-party deposit or trusteeship services for cryptographic keys, in order to guard against accidental loss or destruction of keys, in order to provide for "digital powers of attorney," and so forth.[203] But, although private-sector use of the EES is voluntary, if the EES is used, key escrowing is not "optional." Private-sector users that don't want the escrowing arrangements the government has associated with the EES must look elsewhere.[204] As another example, private-sector users who want to increase the security provided by DES-based technologies can look to "triple-encryption DES," but not to any federal guidance (i.e., a FIPS) in implementing it.

## Executive Branch Implementation of Cryptography Policy

In early 1994, the Clinton Administration announced that it had established an interagency Working Group on Encryption and Telecommunications to implement its encryption policy and review changes as development warrant. The working group is chaired by the Office of Science and Technology Policy (OSTP) and the National Security Council (NSC) and includes representatives of the agencies that participated in the ten-month Presidential review of the impact of encryption technology and advanced digital telecommunications.[205] According to the announcement, the working group will develop recommendations on encryption policies and will ● 'attempt to reconcile the need of privacy and the needs of law enforcement."[206] The group will work with industry to evaluate possible alternatives to the EES. It will work closely with the Information Policy Committee of the Information Infrastructure Task Force and will seek private-sector input both informally and through groups

203 See Parker, op. i,., footnote 9. Parker describes problems that could occur in organizations if cryptography is used w ithout adequate key management and override capabilities by responsible corporate officers. These problems include keys being held for ransom by disgruntled employees and data being rendered inaccessible after being encrypted by employees who then leave to start their ow n company.

204 Use of the technique specified in the EES is not the only means by which a variety of keyholder arrangements can be designed and implemented. See, e.g., David J. Farber, Professor of Telecommunications Systems, Universit y of Pennsylvania, testimony before the Subcommittee on Technology, Environment, and Aviation, Committee on Science, Space, and Technology, U.S. House of Representatives, May 3, 1994, Frank W. Sudia, Bankers Trust Co., "Bankers Trust Company International Corporate Key Escrow, " February 1994; Silvio Micali, MIT Laboratory for Computer Science, "Fair Cryptosystems," MIT/LCS/TR-579.b, November 1993; and Silvio Micah, MIT Laboratory for Computer Science, "Fair Cryptosystems vs. Clipper Chip: A Brief Comparison," Nov. 11, 1993.

The Bankers Trust approach is an alternative key-escrow encryption technique based on general-purpose trusted dev ices and public-key certificates. According to Bankers Trust, it is designed for worldwide business use without requiring government escrow agents.

Micali describes how any public-key cryptosystem can be transformed into a *fair* one that preserves the security and efficiency of the original, while allowing users to select the algorithm they prefer, select all their own secret keys, and use software implementations if desired. *Fair cryptosystems* incorporate a decentralized process for distributing keys to trustees and ensure that court-authorized w ire-tapping ends at the prescribed time. See Silvio Micali, U.S. Patent 5,276,737 (issued Jan. 4, 1994, application filed Apr. 20, 1992) and U.S. Patent 5, 315,658 (issued May 24, 1994, application filed Apr. 19, 1993). The federal government plans to license these patents from Micali (NIST press release. July 11, 1 994)..

205 White House press release, "Working Group on Encryption and Telecommunicatio ns," Feb. 4, 1994. These agencies w ill include the State Department, Justice Department, Commerce Department (including NIST), DOD, the Treasury Department. OMB, NSA, the Federal Bureau of Investigation, and the National Economic Council (ibid.).

206 Ibid.

like the National Security Telecommunications Advisory Committee, CSSPAB, and the Advisory Council on the National Information Infrastructure.

The Clinton Administration made a start at working more closely and more openly with industry through a Key Escrow Encryption Workshop held at NIST on June 10, 1994. The workshop was attended by representatives of many of the leading computer hardware and software companies, as well as attendees from government (including OTA) and academia. One of the assumptions stated as the basis for subsequent action was that, "the results of the deliberations between the government and private sector shall be public] y disclosed, consistent with the national security interests of the country. ''[207] The "proposed action plan" subsequent to the NIST workshop called for:

1. attendees to prepare corporate positions on working with the government to seek "other" approaches to key-escrow encryption. Papers were to be submitted to NIST by July 1, 1994.
2. establishment of joint industry-government working groups (with NIST leadership) to: evaluate all known key-escrowing proposals according to criteria jointly developed by government and industry; hold a public seminar/workshop to discuss and document the results of this analysis; and prepare a report that will be used as the basis of subsequent discussions between "senior government officials and members of the private sector."
3. Other activities, including examination of existing vehicles for collaborative government-industry research and development, development of criteria for determining the suitability of encryption algorithms to be used in conjunction with key escrowing, examination of intellectual-property and royalty issues related to alternative key-escrowing techniques, and creation of a government key-escrowing task force to manage and expedite the search for key-escrow alternatives. The task force would be run by NIST under policy guidance of the interagency working group led by OSTP and NSC.[208]

Based on the discussion and industry presentations at the meeting, there was increasing interest in exploring "other" approaches to key-escrow encryption that can be implemented in software, rather than just in hardware.

On July 20, 1994, acknowledging industry's concerns regarding encryption and export policy, Vice President Al Gore sent a letter to Representative Maria Cantwell that announced a "new phase" of cooperation among government, industry, and privacy advocates. This will include undertaking presidential studies of the effects of U.S. export controls and working with industry to explore alternative types of key-escrow encryption for use in computer networks. Key-escrow encryption based on unclassified algorithms or implemented in software will be among the alternatives to be explored. Escrow-system safeguards, use of nongovernmental key-escrow agents, and liability issues will also be explored. *However, this exploration is in the context of computer and video networks, not telephony; the present EES (Clipper chip) would still be used for telephone systems.*

Additionally, the Advisory Council on the National Information Infrastructure has initiated a "Mega-Project" on privacy, security, and intellectual property will address applications of cryptography as it sets about "defining and setting guidelines for personal privacy and intellectual property protection, outlining methods for protecting First Amendment rights, and for addres-

---

207 "proposed Post Meeting Action Plan," presented at Key Escrow Encryption Workshop, NIST, June IO, 1994 (assumptions).

208 "~)posed Post *Meeting* Action Plan," presented at Key Escrow Encryption Workshop, NIST, Jun. 10,1994 (action plan items 1-3). The NIST contact is Lynn McNulty, NIST Associate Director for Computer Security.

sing national security and emergency preparedness."[209] The Advisory Council and the NII Security Issues Forum held a public meeting on July 15, 1994, to gather input from various user communities regarding their needs and concerns with respect to NII security.

### *Key Escrowing for the EES*

In the meantime, however, the Clinton Administration is investing in implementing key escrowing and the EES. In early 1994, NIST estimated it would take $14 million to establish the escrow system and $16 million in annual operating costs for the two agents.[210] Justice Department purchases of EES equipment were estimated at $12.5 million.[211]

NIST is the program manager for key escrowing; the Department of Justice and the Federal Bureau of Investigation are family-key agents (the EES family key is used to encrypt the law enforcement access field).[212] In February 1994, Attorney General Reno designated NIST and Treasury's Automated Systems Division as the escrow agents for the EES (Clipper) chip-specific keys needed to gain access to encrypted communications. The Vice President reportedly deemed this an "interim solution," recognizing that having both escrow agents within the executive branch does little to quell concerns over the potential for misuse of the escrowing system. The Clinton Administration reportedly has been considering using private organizations or an office in the court system as agents.[213] By June 1994, NIST had escrowed 17,000 Clipper chip keys and was preparing for escrowing of *Capstone* chip keys.[214]

The Administration is developing auditing and accountability controls to prevent misuse of keys (during programming of the chips or in the escrow agencies) and to increase public confidence. According to NIST, these physical-security and institutional controls include:

- magnetically "wiping" computer memories;
- locking computers in secure facilities;
- using cleared staff;
- using shrink-wrapped software;
- using safes and secure areas to store programmed EES chips and key components;
- packaging key components in tamper-evident security packaging, with serial numbers;
- logging when key components are placed in and removed from safes;
- using "dual controls" for two-person security, requiring two individuals to get at an escrowed key component;
- using split knowledge—two escrow agents each have one of the two key components;
- using redundancy in storage and transportation of key components;
- encrypting stored key components at each site; and
- ensuring that key components never appear in the clear outside of a computer—the escrow agents never see them.[215]

---

209 National Information Infrastructure Advisory Council announcement, Apr. 25, 1994.

210 *Federal Register*, vol 59, Feb. 9, 1994, pp. 1 I -12. OTA asked for, but did not receive, any subsequent cost figures.

211 Roger Callahan, op. cit., footnote 182, point 52.

212 Miles Smid, N] ST, "The U.S. Government Key Escrow System," presentation at NIST Key Escrow Encryption Workshop, June 10, 1993.

213 See Brad Bass, "'White House To Pick Third Party To Hold One Set of Decryption Keys," *Federal Computer Week*, Mar. 28, 1994, p. 3; and Kevin Power, "Exactly Who Will Guard Those Data Encryption Keys'?" *Government Computer News*, Apr. 18, 1994, p. IO.

214 Miles Smid, Manager, Security Technology Group, N] ST, personal communication, May 25, 1994; and Miles Smid, op. cit., footnote 212, June 10, 1994. See also Dorothy E. Denning and Miles Smid, "Key Escrowing Today," *IEEE Communications*, in press (September 1994).

215 Ibid.

A June 1994 NIST summary of key-escrow program activities included: preparation for programming of Capstone chips, modification of the Secure Hash Algorithm to include the technical correction announced in April 1994, search for a possible new escrow agent, and review of "target system" requirements for the key-escrowing system. As of June 1994, according to NIST, the interim key-escrowing system was using prototype components, research and development software, and a combination of manual and automated operations.

The "target" key-escrowing system will have an upgraded chip programming facility, use cryptographic functions to automate key transportation, develop a trusted escrow agent workstation, and complete a trusted decryption processor.[216] According to NIST, the key-escrow program is in the second of four phases of development. Phase 1 (September 1993 through March 1994) saw establishment of a prototype chip programming facility and manual procedures for handling and storage of escrow components; there was no decryption processor. In phase 2 (April 1994— ), there is a prototype decryption processor, a simple key-component extraction program, and manual key-component release procedures. Phase 3 will see the first release of a target chip programming facility and an escrow-agent workstation; phase 4 will see deployment of the final operating capability for all escrowing subsystems.[217]

Although these facilities, procedures, and security measures have been developed specifically for the EES and other implementations of the SKIPJACK key-escrow encryption algorithm, they could be made applicable to other forms of escrowed encryption, including software-based key-escrow approaches. Some of the established procedures and security measures would have to be modified and/or augmented for software-based escrowed encryption. For encryption (of any type) implemented in software, the integrity and reliability of the software program and code is of paramount importance.

## STRATEGIC AND TACTICAL CONGRESSIONAL ROLES

Congress has vital strategic roles in cryptography policy and, more generally, in safeguarding information and protecting personal privacy in a networked society. This chapter has examined these issues as they relate to federal safeguard standards and to agency roles in safeguarding information. Other controversies--current ones like digital telephony and future ones regarding electronic cash and commerce—will involve similar issues and can be dealt with within a sufficiently broad strategic framework.

Cryptography is a fundamental tool for safeguarding information and, therefore, it has become a technology of broad application. Despite the growth in nongovernmental cryptographic research and safeguard development over the past 20 years, the federal government still has the most expertise in cryptography and cryptanalysts. Thus, federal standards (the FIPS) have substantial significance for the development and use of these technologies. The nongovernmental market for cryptography products has grown in the last 20 years or so, but is still developing. Export controls also have substantial significance for the development and use of these technologies.

Therefore, Congress's choices in setting national cryptography policies (including standards and export controls) affect information security and privacy in society as a whole. Congress has an even more direct role in establishing the policy guidance within which federal agencies safeguard information, and in oversight of agency and OMB measures to implement information security and privacy requirements. This section presents options for congressional consideration with respect to safeguarding information in federal agencies

---

[216] Miles Smid, op. cit., footnote 212, June 10, 1994.

[217] Ibid.

and to national cryptography policy. Congress has both strategic and tactical options in dealing with cryptography.

## The Need for More Open Processes

More open policies and processes can be used to increase equity and acceptance in implementing cryptography and other technologies. The current controversies over cryptography can be characterized in terms of tensions between the government and individuals. They center on the issue of trust in government. Trust is a particular issue in cases like cryptography, when national-security concerns require an asymmetry of information between the government and the public. Government initiatives of broad public application, formulated in secret and executed without legislation, naturally give rise to concerns over their intent and application. There is a history of concern over use of presidential national-security directives-often classified and not publicly released[218]—to make and execute policy:

> Implementation of policy decisions through the issuance of undisclosed directives poses a significant threat to Congress' ability to discharge its legislative and oversight responsibilities under the Constitution. Operational activities undertaken beyond the purview of the Congress foster a grave risk of the creation of an unaccountable shadow government-a development that would be inconsistent with the principles underlying our republic.[219]

The process by which the EES was selected and approved was closed to those outside the executive branch. Furthermore, the institutional and procedural means by which the EES is being deployed (such as the escrow management procedures) continue to be developed in a closed forum. In May 1994 testimony before the House Subcommittee on Technology, Environment, and Aviation, David Farber (University of Pennsylvania) stated that "open technical processes are best for solving hard problems," such as the need for technology and public policy that:

> . . . assure[s] privacy and security, enables law enforcement to continue to do its job, and, at the same time, respects fundamental civil liberties which are at the heart of our constitutional system of government.[220]

Farber called for a more open process for evolving proposals like the EES:

> While I recognize that a small part of cryptography will always be classified, most of the development of the proposed escrow system has been taking place in those room[s] (not smoke-filled any more). This process must be brought out into the sunshine of the technical and policy community. Proposals like Clipper must be evolved, if they are to have any chance of success, with the co-operation and understanding of the industrial and academic community and their enthusiastic cooperation rather than their mistrust. This penchant for openness must not be seen as a power struggle between industry and government, or as an excuse for revisiting a decision that technologists dislike for political reasons. Rather it is a reflection of a deep faith in open design processes and a recognition that closed processes invariably lead to solutions which are too narrow and don't last.[221]

In calling for congressional action to ensure that overall cryptography policy is developed in a broader context, Jerry Berman of the Electronic Frontier Foundation (EFF) testified that Congress should seek the implementation of a set of public

---

218 H. Rept. 100-153, Part II, op. Cit., footnote 33, pp. 31-33. For example, the Congressional Research Service (CRS) reported to the House Committee on Government Operations that, between 1981 and 1987, over 200 National Security Decision Directives (NSDDs) had been issued by the Reagan Administration, and only five had been publicly disclosed. According to CRS, the NSDDs comprised an ongoing system of declared (but usually secret ) U.S. policy statements that, even when available to the public, had to be requested in writing and were not published in the *Federal Register* (ibid.). NSDD-145 was one of the directives issued during this period.

219 H. Rept. 100-153, Part 11, op. cit., footnote 33, p. 33.

220 Farber testimony, op. cit., footnote 204, p. 4.

221 Ibid., p. 5.

policies that would promote the widespread availability of cryptographic systems that seek "reasonable" cooperation with law enforcement and national security needs; promote constitutional rights of privacy and adhere to traditional, Fourth Amendment search and seizure rules; and maintain civilian control over public computer and communications security, in accordance with the Computer Security Act of 1987.[222]

### The CSSPAB's Call for a Broad Review of Cryptography

In early 1992, prompted by controversies over the proposed DSS, the Computer System Security and Privacy Advisory Board advised NIST to delay a decision on adopting a signature standard pending a broad national review on the uses of cryptography.[223] Noting the significant public policy issues raised during review of the proposed signature standard, the CSSPAB unanimously approved a resolution to the effect that "a national level public review of the positive and negative implications of the widespread use of public and secret key cryptography is required" in order to produce a "national policy concerning the use of cryptography in unclassified/sensitive government and the private sector. ''224

After the escrowed-encryption initiative was announced by President Clinton in April 1993—a complete surprise to the CSSPAB—the Board was asked by the Deputy Director of NIST to devote its June 1993 meeting to hearing public views on what was being called the Clipper program,[225] The Board then unanimously resolved to gather additional public and government input. The Board recommended that the interagency cryptography policy review that was part of the President's April 1993 announcement take note of the "serious concerns and problems" the CSSPAB had identified.[226] The CSSPAB subsequently held four more days of public hearings and resolved (not unanimously) that the preliminary concerns identified in the June hearings had been "confirmed as serious concerns which need to be resolved." 227 The Board strengthened its views on the importance of a broad national cryptography policy review, including Congress, before any new or additional cryptographic "solution" is approved as a U.S. government standard, in order to resolve the following issues:

1. the protection of law-enforcement and national-security interests;

---

222 Jerry J. Berman, Executive Director, Electronic Frontier Foundation, testimony before the Subcommittee on Technology, Environment, and Aviation, Committee on Science, Space, and Technology, U.S. House of Representatives, May 3, 1994, pp. 13-14.

223 Minutes of the March 17-18, 1992 meeting of the CSSPAB (available from NIST). See also David K. Black, op. cit., pp. 439-440; Darryl K. Taft, "Board Finds NIST's DSS Unacceptable," *Government Computer News, Dec. 23, 1991,* pp. 1, 56; and Kevin Power, "Security Board Calls for Delay on Digital Signature," *Government Computer News,* Mar. 30, 992, p. 114. In the public comments, negative responses outnumbered endorsements of the DSS by 90 to 13 (Power, ibid.).

224 CSSPAB Resolution No 1 of Mar 18 1992. See discussion of this resolution and other CSSPAB activities in: Willis H. Ware, Chairman, CSSPAB, testimony before the Subcommittee on Technology, Environment, and Aviation, Committee on Science, Space, and Technology, U.S. House of Representatives, May 3, 1994.

225 See Ware testimony, ibid., pp. 6-7. See also "Cryptographic Issue Statements," submitted to the Computer System Security and privacy Advisory Board, revised June 25, 1993 (available from NIST) and "Summary of Comments Received by the Computer System Security and Privacy Advisory Board (in conjunction with its June 2-4, 1993 public meeting)," also available from N] ST. A full transcript is also available from NIST.

226 CSSPAB Resolution No. 1 of June 4, 1993 and attachment. The Board noted that Congress should also play a role in the conduct and approval of the results of the review.

227 CSSPAB Resolution 93-5 of Sept. 1-2, 1993.

2. the protection of U.S. computer and telecommunications interests in the international marketplace; and
3. the protection of U.S. persons' interests, both domestically and internationally.[228]

This resolution stated that, ". ., the Congress of the U.S. must be involved in the establishment of cryptographic policy.''[229]

In May 1994 testimony, CSSPAB Chairman Willis Ware of the RAND Corp. noted that, from March 1992 to present, based on its publicly available record, the board has:

- focused attention of government agencies on the cryptographic issue;
- focused attention of the public and various private-sector organizations on the cryptographic issues;
- provided a forum in which public views as well as government views could be heard;
- assembled the only public record of ongoing activities and progress in the Clipper initiative; and
- created a public record for national cryptography policy, and its many dimensions—Clipper, Capstone [OTA note: these refer to implementations of the EES encryption algorithm], the DSS, public concerns, constitutional concerns.[230]

### The National Research Council Study

The Committees on Armed Services, Commerce, Intelligence, and Judiciary have asked the National Research Council (NRC) to undertake a two-year study of national policy with respect to the use and regulation of cryptography. 23] The study is intended to address how technology affects the policy options for various national interests (e.g., economic competitiveness with respect to export controls, national security, law enforcement, and individual privacy rights) and the process by which national cryptography policy has been formulated. It will also address the current and future capabilities of cryptographic technologies suitable for commercial use. In its Resolution 93-7, the CSSPAB endorsed the NRC study of national cryptography as the study that ● 'best accomplishes" the Board's "repeated calls" for a national review.[232]

In June 1994, the NRC was still forming the study committee; the chair and vice-chair had been selected. According to the study staff, once the committee process is fully under way, the committee will be soliciting the views of and input from as wide a constituency as possible; the committee hopes that those with interests in the topic will respond to calls for input '*with thought and deliberation.''[233] A subpanel of the committee will receive security clearance; the role of this subpanel will be to ensure that the findings of the study committee are ● 'consistent with what is known in the classified world. ''234

## National Cryptography Policy

Congress has a major role in establishing the nation's cryptography policy. Just as cryptography has become a technology of broad application, so will decisions about cryptography policy have in-

228 CSSPAB Resolution 93-6 of Sept.1-2,1993.

229 Ibid. See also Ware testimony, op. cit., footnote 224.

230 Ware testimony, i bid., p. 11,

231 As part of the Defense Authorization Bill for FY 1994 (Public Law 103- 160). the Committees on Armed Services, Intelligence, Commerce, and Judiciary of the Senate and House of Representatives have asked the National Research Council to undertake a classified, two-year study of national policy with respect to the use and regulation of cryptography. Announcement from the Computer Science and Telecommunications Board, National Research Council, Dec. 7, 1993.

232 CSSPAB Resolution 93-7 (Dec. 8-9, 1993).

233 Herb Lin, Senior Staff Officer, National Research Council, personal communications, May 1 I and June 1, 1994.

234 Ibid.

creasingly broad effects on society. The effects of policies about cryptography are not limited to technological developments in cryptography, or even to the health and vitality of companies that produce or use products incorporating cryptography. Instead, these policies will increasingly affect the everyday lives of most Americans. Cryptography will be used to help ensure the confidentiality and integrity of health records and tax returns. It will help speed the way to electronic commerce, and it will help manage copyrighted material in electronic form.

Recognizing the importance of the technology and the policies that govern its development, dissemination, and use, Congress asked the NRC to conduct a major study that would support a broad review of cryptography (see above). The results of the study are expected to be available in 1996. ***Given the speed with which the Administration is acting, information to support a Congressional policy review of cryptography is out of phase with the implementation of key-escrow encryption. Therefore, Congress may wish to consider placing a hold on further deployment of key-escrow encryption, pending a congressional policy review.***

An important outcome of a broad review of national cryptography policy would be development of more open processes to determine how cryptography will be deployed throughout society. This deployment includes development of the public-key infrastructures and certification authorities that will support electronic delivery of government services, copyright management, and digital commerce (see chapters 2 and 3). More open processes would build trust and confidence in government operations and leadership. More openness would also allow diverse stakeholders to understand how their views and concerns were being balanced with those of others, in establishing an equitable deployment of these technologies, even when some of the specifics of the technology remain classified. More open processes will also allow for public consensus-building, providing better information for use in congressional oversight of agency activities. ***Toward this end, Congress may wish to consider the extent to which the current working relationship between NIST and NSA will be a satisfactory part of this open process, or the extent to which the current arrangements should be reevaluated and revised.***

***Another important outcome would be a sense of Congress with regard to information policy and technology and to when the impact of certain technologies is so pervasive and powerful that legislation is needed to provide public visibility and accountability.*** For example, many of the concerns surrounding the EES (and the key-escrowing initiative in general) focus on whether key-escrow encryption will be made mandatory for government agencies or the private sector, or if nonescrowed encryption will be banned, and/or if these actions could be taken without legislation,

Other concerns focus on whether or not alternative forms of encryption would be available that would allow private individuals and organizations the option of depositing keys with one or more third-party trustees, or not—at their discretion. These trustees might be within government, or in the private sector, depending on the nature of the information to be safeguarded and the identity of its custodians. (For example, federal policy might require agencies to deposit cryptographic keys used to maintain confidentiality of taxpayer data only with government trustees. Companies and individuals might be free not to use trustees, or if they did, could choose third-party trustees in the private sector or use the services of a government trustee.) The NRC study should be valuable in helping Congress to understand the broad range of technical and institutional alternatives available for various types of trusteeships for cryptographic keys, "digital powers of attorney," and the like. However, if implementation of the EES and related technologies continues at the current pace, key-escrow encryption may already be embedded in information systems.

***As part of a broad national cryptography policy, Congress may wish to periodically examine export controls on cryptography, to ensure that these continue to reflect an appropriate balance between the needs of signals intelligence and law enforcement and the needs of the public and business communities. This ex-***

***amination would take into account changes in foreign capabilities and foreign availability of cryptographic technologies.*** Information from industry on the results of licensing reforms and the executive branch study of the encryption market and export controls that is included in the 1994 export administration legislation (see discussion above on export controls and competitiveness) should provide some near-term information. ***However, the scope and methodology of the studies that Congress might wish to use in the future may differ from these. Congress might wish to assess the validity and effectiveness of the Administration's studies by conducting oversight hearings, by undertaking a staff analysis, or by requesting a study from the Congressional Budget Office.***

### *Congressional Responses to Escrowed-Encryption Initiatives*

Congress also has a more near-term role to play in determining the extent to which—and how—the EES and other escrowed-encryption systems will be deployed in the United States. These actions can be taken within a long-term, strategic framework. Congressional oversight of the effectiveness of policy measures and controls can allow Congress to revisit these issues as needed, or as the consequences of previous decisions become more apparent.

The EES was issued as a voluntary federal standard; use of the EES by the private sector is also voluntary. The Clinton Administration has stated that it has no plans to make escrowed encryption mandatory, or to ban other forms of encryption:

> As the [Clinton] Administration has made clear on a number of occasions, the key-escrow encryption initiative is a voluntary one; we have absolutely no intention of mandating private use of a particular kind of cryptography, nor of criminalizing the private use of certain kinds of cryptography. We are confident, however, of the quality and strength of key-escrow encryption as embodied in this chip [i.e., the Clipper chip implementation of EES], and we believe it will become increasingly attractive to the private sector as an excellent, easy-to-use method of protecting sensitive personal and business information.[235]

But, absent legislation, these intentions are not binding for future administrations and also leave open the question of what will happen if EES and related technologies do not prove attractive to the private sector. Moreover, the executive branch may soon be using the EES and/or related escrowed-encryption technologies to safeguard—among other things—large volumes of private information about individuals (e.g., taxpayer data, healthcare information, and so forth).

For these reasons, the EES and other key-escrowing initiatives are by no means only an executive branch concern. The EES and any subsequent escrowed-encryption standards also warrant congressional attention because of the public funds that will be spent in deploying them. Moreover, negative public perceptions of the EES and the processes by which encryption standards are developed and deployed may erode public confidence and trust in government and, consequently, the effectiveness of federal leadership in promoting responsible safeguard use.

In his May 1994 testimony before the Senate Subcommittee on Technology and the Law, Whitfield Diffie observed that:

> In my experience, the people who support the key escrow initiative are inclined to express substantial trust in the government. I find it ironic therefore that in its conduct of this program, the [Clinton] Administration has followed a course that could hardly have been better designed to provoke distrust. The introduction of mechanisms designed to assure the government's ability to conduct electronic surveillance on its citizens and limit the ability of citizens to protect themselves against such surveillance is a major policy decision of the information age. It has been presented, however, as a technicality, buried in an obscure series of regulations. In so

[235] Jo Ann Hams testimony, op. cit., footnote 8, p. 3.

doing, it has avoided congressional consideration of either its objectives or its budget. The underlying secrecy of the technology has been used as a tool for doling out information piecemeal and making a timely understanding of the issues difficult to achieve.[236]

***In responding to the Clinton Administration's escrowed-encryption initiatives, and in determining the extent to which appropriated funds should be used in implementing EES and related technologies, Congress might wish toaddress the appropriate locations of the key-escrow agents, particularly for federal agencies, before additional investments are made in staff and facilities for them. Public acceptance of key-escrow encryption might be improved-but not assured--by an escrowing system that used separation of powers to reduce perceptions of the potential for misuse.***

In response to an OTA inquiry in late 1993, the Congressional Research Service examined any constitutional problems that might arise in placing an escrow agent elsewhere in government. According to CRS, placing custody of one set of keys in a federal court or an agency of the judicial branch would almost certainly pass constitutional challenge:

> First, as we discussed, it is a foregone conclusion that custody of one key could not be vested in Congress, a congressional agency, or a congressional agent. Using strict separation-of-powers standards, the Supreme Court has held that no legislator or agency or agent of the Legislative Branch may be given a role in execution of the laws. . . Custody of one of the keys and the attendant duties flowing from that possession is certainly execution of the laws.
>
> Second, placing custody of one of the keys in a federal court or in an agency of the Judicial Branch almost certainly pass constitutional challenge. . .
>
> Under the Fourth Amendment, it is the responsibility of judges to issue warrants for searches and seizures, including warrants for wiretapping and other electronic surveillance. Courts will authorize interceptions of the telecommunications at issue here. Under those circumstances, it is difficult to see a successful argument that custody of one of the keys [is] constitutionally inappropriately placed in a judicial agency.
>
> Alternatively, it would seem equally valid to place custody in a court itself. . . If a court is to issue a warrant authorizing seizure and decryption of certain telecommunications, effectuation of such a warrant through the partial agency of one of two encryption keys hardly seems to stray beyond the bounds of judicial cognizance.[237]

***With respect to current and subsequent escrowed-encryption initiatives, and in determining the extent to which appropriated funds should be used in implementing EES and related technologies, Congress may wish to address the issue of criminal penalties for misuse and unauthorized disclosure of escrowed key components. Congress may also wish to consider allowing damages to be awarded for individuals or organizations who were harmed by misuse or unauthorized disclosure of escrowed key components.***

Acceptance in the United States, at least, might be improved if criminal penalties were associated with misuse of escrowed keys[238] and if damages could be awarded to individuals or organizations harmed by misuse of escrowed keys. In May 1994 testimony before the House Subcommittee on Technology, Environment, and Aviation, Jerry Berman of the Electronic Frontier Foundation

---

236 Diffie testimony, op. cit., footnote 24, p.10.

237 Johnny H. Killian, Senior Specialist, American Constitutional Law, CRS, "Options for Deposit of Encryption Key Used in Certain Electronic Interceptions Outside Executive Branch," memorandum to Joan D. Winston, OTA, Mar. 3, 1994,

238 The current statutes regarding computer fraud and abuse, counterfeit access devices, and trafficking in passwords (i.e., 18 USC 1029, 1030) might conceivably be stretched to cover some misuses by escrow agents, but are not sufficient.

noted that the lack of legal rights for those whose keys were escrowed and lack of stability in escrow rules served to reduce trust in the system:

> As currently written, the escrow procedures insulate the government escrow agents from any legal liability for unauthorized or negligent release of an individual's key. This is contrary to the very notion of a escrow system, which ordinarily would provide a legal remedy for the depositor whose deposit is released without authorization. If anything, escrow agents should be subject to strict liability for unauthorized disclosure of keys.
>
> The Administration has specifically stated that it will not seek to have the escrow procedures incorporated into legislation or official regulations. Without formalization of rules, users have no guaranty that subsequent administrations will follow the same rules or offer users the same degree of protection. This will greatly reduce trust in the system.[239]

However, while measures addressing the location of the escrow agents, sanctions, and liability for key-escrow encryption could increase acceptance of escrowed encryption in the United States, these measures would not be sufficient to ensure acceptance in the international business community.[240] Other aspects of key-escrow encryption, such as use of a classified encryption algorithm, implementation in hardware only, and key management, could still be troublesome to the international business community (see below).

The International Chamber of Commerce's (ICC) ICC *Position Paper on International Encryption Policy* notes the growing importance of cryptography in securing business information and transactions on an international basis and, therefore, the significance of restrictions and controls on encryption methods:

> While the ICC recognises that governments have a national security responsibility, it cannot over-emphasise the importance of avoiding artificial obstacles to trade through restrictions and controls on Encryption Methods. Many countries have or may use a variety of restrictions which inhibit businesses from employing secure communications. These restrictions include export and import control laws, usage restrictions, restrictive licensing arrangements, etc. These diverse, restrictive measures create an international environment which does not permit businesses to acquire, use, store, or sell Encryption Methods uniformly to secure their worldwide communications.
>
> ...What is needed is an international policy which minimises unnecessary barriers between countries and which creates a broader international awareness of the sensitive nature of information
>
> .... Furthermore, the ICC believes that restriction in the use of encryption for [crime prevention] would be questionable given that those engaged in criminal activities would most certainly not feel compelled to comply with the regulations applied to the general business community. The ICC would urge governments not to adopt a restrictive approach which would place a particularly onerous burden on business and society as a whole.[241]

ICC's position paper calls on governments to: 1 ) remove unnecessary export and import controls, usage restrictions, restrictive licensing arrangements and the like on encryption methods used in commercial applications; 2) enable network interoperability by encouraging global standardization; 3) maximize users' freedom of choice; and 4) work together with industry to resolve barriers by jointly developing a comprehensive international policy on encryption.

ICC recommends that global encryption policy be based on the following broad principles:

---

239 Berman testimony, op. cit, footnote 222, p. 5.

240 Nanette DiTosto, Manager, Telecommunications/Economic and Financial Policy, U.S. Council for International Business, personal communication, Apr. 28, 1994. Among its other activities, the Council is the U.S. affiliate of the International Chamber of Commerce.

241 International Chamber of Commerce, ICC *Positron Paper on International Encryption Policy* (Paris: ICC, 1994), pp. 2,3.

. Different encryption methods will be needed to fulfill a variety of user needs. Users should be free to use and implement the already existing framework of generally available and generally accepted encryption methods and to choose keys and key management without restrictions. Cryptographic algorithms and key-management schemes must be open to public scrutiny for the commercial sector to gain the necessary level of confidence in them.

- Commercial users, vendors, and governments should work together in an open international forum in preparing and approving global standards.

. Both hardware and software implementations of encryption methods should be allowed. Vendors and users should be free to make technical and economic choices about modes of implementation and operation.

. Owners, providers, and users of encryption methods should agree on the responsibility, accountability, and liability for such methods.

. With the exception of encryption methods specifically developed for military or diplomatic uses, encryption methods should not be subject to export or import controls, usage restrictions, restrictive licensing arrangements, or other restrictions.[242]

In June 1994, the U.S. Public Policy Committee of the Association for Computing Machinery (USACM) issued its position on the EES and released a special panel report on issues in U.S. cryptography policy.[243] The USACM recommended, among other things, that the process of developing the FIPS be placed under the Administrative Procedures Act, reflecting their impact on nonfederal organizations and the public at large.[244]

## Safeguarding Information in Federal Agencies

The forthcoming revision of Appendix 111 ("Agency Security Plans") of OMB Circular A-130 should lead to improved federal information-security practices. According to OMB, the revision of Appendix III will take into account the provisions and intent of the Computer Security Act of 1987, as well as observations regarding agency security plans and practices from agency visits. To the extent that the revised Appendix III facilitates more uniform treatment across agencies, it can also make fulfillment of Computer Security Act and Privacy Act requirements more effective with respect to data sharing and secondary uses (see discussion in chapter 3).

The revised Appendix 111 had not been issued by the time this report was completed. Although OTA discussed information security and privacy issues with OMB staff during interviews and a December 1993 OTA workshop, OTA did not have access to a draft of the revised security appendix. Therefore, OTA was unable to assess the revision's potential for improving information security in federal agencies, for holding agency managers accountable for security, or for ensuring uniform protection in light of data sharing and secondary uses.

***After the revised Appendix III of OMB Circular A-130 is issued, Congress may wish to assess the effectiveness of the OMB's revised guidelines, including improvements in implementing the Computer Security Act's provisions regarding agency security plans and training, in order to determine whether additional statutory requirements or oversight measures are needed. This might be accomplished by conducting oversight hearings, undertaking a staff analysis, ana/or requesting a study from the General Ac-***

---

242 Ibid., pp. 3-4.

243 Landau et al., op. cit., footnote 6.

244 USACM position on the Escrowed Encryption Standard, June 30, 1994.

***counting Office.*** However, the effects of OMB's revised guidance may not be apparent for some time after the revised Appendix III is issued. Therefore, a few years may pass before GAO is able to report government-wide findings that would be the basis for determining the need for further revision or legislation.

***In the interim, Congress might wish to gain additional insight through hearings to gauge the reaction of agencies, as well as privacy and security experts from outside government, to OMB's revised guidelines. Oversight of this sort might be especially valuable for agencies, such as the Internal Revenue Service, that are developing major new information systems.***

***In the course of its oversight and when considering the direction of any new legislation, Congress might wish to consider measures to:***

- ***ensure that agencies include explicit provisions for safeguarding information assets in any information-technology planning documents;***
- ***ensure that agencies budget sufficient resources to safeguard information assets, whether as a percentage of information-technology modernization and/or operating budgets, or otherwise;*** *and/or*
- *ensure that the Department of Commerce assigns sufficient resources to NIST to support its Computer Security Act responsibilities, as well as NIST's other activities related to safeguarding information and protecting privacy in networks.*

Regarding NIST's computer-security budget (see table 4-1 ), OTA has not determined the extent to which additional funding is needed, or the extent to which additional funding would improve the overall effectiveness of NIST's information-security activities. However, in staff discussions and workshops, individuals from outside and within government repeatedly noted that NIST's security activities were not proactive and that NIST often lagged in providing useful and needed standards and guidelines.[245] Many individuals from the private sector felt that NIST's limited resources for security activities precluded NIST from doing work that would also be useful to industry. Additional resources, whether from overall increases in NIST's budget and/or from formation of a new Information Technology Laboratory, could enhance NIST's technical capabilities, enable it to be more proactive, and hence, be more useful to federal agencies and to industry.

NIST activities with respect to standards and guidelines related to cryptography are a special case, however. Increased funding alone will not be sufficient to ensure NIST's technological leadership or its fulfillment of the "balancing" role as envisioned by the Computer Security Act of 1987. With respect to cryptography, national-security constraints set forth in executive branch policy directives appear to be binding, implemented through executive branch coordinating mechanisms including those set forth in the NIST/NSA memorandum of understanding. These constraints have resulted, for example, in the closed processes by which the Administration's key-escrow encryption initiatives, including the EES, have been developed and implemented. Increased funding could enable NIST to become a more equal partner to NSA, at least in deploying (if not developing) cryptographic standards. But, if NIST/NSA processes and outcomes are to reflect a different balance of national security and other public interests, or more openness, than has been evidenced over the past five years, clear policy guidance and oversight will be needed.

[245] For a sample of federal-agency "wants and ideas" regarding NIST's role, see Gilbert, op. cit., footnote 163, appendix M, especially pp. appendix-85 and appendix-86.