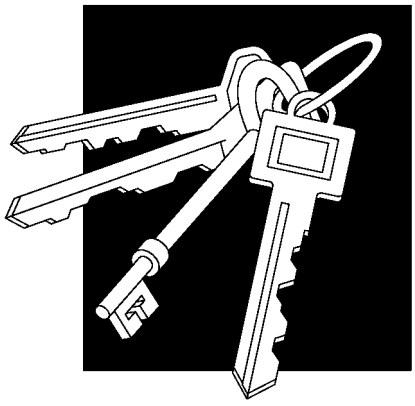
Introduction and Summary 1

Controversies, problems, and proposed solutions related to information security and privacy are becoming increasingly prominent among government, business, academia, and the general public. At the same time, use of information networks for business has continued to expand, and ventures to bring electronic commerce and "electronic cash" into homes and offices are materializing rapidly.[1] Government agencies have continued to expand both the scale and scope of their network connectivities; information technologies and networks are featured prominently in plans to make government more efficient, effective, and responsive.[2]

Until recently, topics such as intrusion countermeasures for computer networks or the merits of particular encryption techniques were mostly of interest to specialists. However, in the past



[1] See, e.g., Randy Barrett, "Hauling in the Network—Behind the World's Digital Cash Curve," *Washington Technology*, Oct. 27, 1994, p. 18; Neil Munro, "Branch Banks Go Way of the Drive-In," *Washington Technology*, Feb. 23, 1995, pp. 1,48; Amy Cortese et al., "Cashing In on Cyberspace: A Rush of Software Development To Create an Electronic Marketplace," *Business Week*, Feb. 27, 1995, pp. 78-86; Bob Metcalfe, "Internet Digital Cash—Don't Leave Your Home Page Without It," *InfoWorld*, Mar. 13, 1995, p. 55; "Netscape Signs Up 19 Users for Its System of Internet Security," *The Wall Street Journal*, Mar. 20, 1995, p. B3; Saul Hansell, "VISA Will Put a Microchip in New Cards—Product Is Designed for Small Purchases," *The New York Times*, Mar. 21, 1995, p. D3; Jorgen Wouters, "Brother, Can You Spare a Virtual Dime?" *Washington Technology*, Mar. 23, 1995, pp. 1, 44.

[2] See, e.g., Neil Munro, "Feds May Get New Infotech Executive," *Washington Technology*, Feb. 23, 1995, pp. 1, 49; Charles A. Bowsher, Comptroller General of the United States, "Government Reform: Using Reengineering and Technology To Improve Government Performance," GAO/T-OCG-95-2, testimony before the Committee on Governmental Affairs, U.S. Senate, Feb. 2, 1995; and Elena Varon, "Reinventing Is Old Hat for New Chairman," *Federal Computer Week*, Feb. 20, 1995, pp. 22, 27.

few years, stories about controversial federal encryption standards, "password sniffing" and unauthorized intrusions on the Internet, the pursuit and capture of a notorious computer "cracker," and export controls on computer programs that perform encryption have become front-page news.[3]

The increased visibility and importance accorded information security and privacy protection (see box 1-1) reflect a number of institutional, social, and technological changes that have made information technologies critical parts of daily life.[4] We are in transition to a society that is becoming critically dependent on electronic information and network connectivity. This is exemplified by the explosive growth of the Internet, which now has host computers in over 85 countries, as well as the rapidly expanding variety of online sources of information, services, and entertainment. The growing dependence of both the public and private sectors on electronic information and networking makes the ability to safeguard information and provide adequate privacy protections for individuals absolutely essential.

In September 1994, the Office of Technology Assessment (OTA) released the report *Information Security and Privacy in Network Environments* (see box 1-2).[5] That report was prepared in response to a request by the Senate Committee on Governmental Affairs and the House Subcommittee on Telecommunications and Finance. The need for congressional attention to safeguarding unclassified information has been reinforced in the months since the release of the OTA report.

INTRODUCTION

This background paper is part of OTA's follow-on assistance to the Senate Committee on Governmental Affairs after the September 1994 OTA report on information security and privacy. The Committee had requested additional informational and analytical assistance from OTA in order to prepare for hearings and legislation in the 104th Congress (see the letter of request in appendix A).

This background paper is a companion and supplement to the 1994 report and is intended to be used in conjunction with it. For the reader's convenience, however, pertinent technical and institutional background material, drawn from that report and updated where possible, is included in this background in appendices B ("Federal Information Security and the Computer Security Act"), C ("U.S. Export Controls on Cryptography"), and D ("Summary of Issues and Options from the 1994 OTA Report").

One purpose of this background paper is to is to update some key issues that OTA had identified in the report, in light of recent developments. Another purpose is to develop further some of OTA's findings and options, particularly as these relate to the effects of government policies on the private

---

[3] See John Markoff, "Flaw Discovered in Federal Plan for Wiretapping," *The New York Times*, June 2, 1994, pp. 1, D17; Peter H. Lewis, "Hackers on Internet Posing Security Risks, Experts Say," *The New York Times*, July 21, 1994, pp. 1, B10; John Markoff, "A Most-Wanted Cyberthief Is Caught in His Own Web," *The New York Times*, Feb. 16, 1995, pp. 1, D17; and John Schwartz, "Privacy Program: An On-Line Weapon?" *The Washington Post*, Apr. 3, 1995, pp. A1, A13. See also Jared Sandberg, "Newest Security Glitch on the Internet Could Affect Many 'Host' Computers," *The Wall Street Journal*, Feb. 23, 1995, p. B8; Jared Sandberg, "Immorality Play: Acclaiming Hackers as Heroes," *The Wall Street Journal*, Feb. 27, 1995, p. B1, B8; and Amy Cortese et al., "Warding Off the Cyberspace Invaders," *Business Week*, Mar. 13, 1995, pp. 92-93.

[4] See U.S. Congress, Office of Technology Assessment, *Making Government Work: Electronic Delivery of Government Services*, OTA-TCT-578 (Washington, DC: U.S. Government Printing Office, September 1993); *Electronic Enterprises: Looking to the Future*, OTA-TCT-600 578 (Washington, DC: U.S. Government Printing Office, May 1994); and *Wireless Technologies and the National Information Infrastructure* (forthcoming, 1995). See also U.S. General Accounting Office, *Information Superhighway: An Overview of Technology Challenges*, GAO/AIMD-95-23 (Washington, DC: U.S. General Accounting Office, January 1995).

[5] U.S. Congress, Office of Technology Assessment, *Information Security and Privacy in Network Environments*, OTA-TCT-606 (Washington, DC: U.S. Government Printing Office, September 1994). Available from OTA Online via anonymous file transfer protocol (ftp://otabbs.ota.gov/pub/information.security/) or World Wide Web (http://www.ota.gov).

BOX 1-1: Some Notes on Terminology

Information Security

There are three main aspects of information security: 1) confidentiality, 2) integrity, and 3) availability These protect against the unauthorized disclosure, modification, or destruction of information. The focus of this background paper, and the OTA report *Information Security and Privacy in Network Environments* (September 1994) that it supplements, is technical and institutional measures to ensure the confidentiality and integrity of unclassified electronic *Information* in networks, not the security of the networks themselves. Network reliability and survivability (related to '(availability") were not addressed; these topics are expected to be the focus of subsequent OTA work.

Confidentiality and Privacy

OTA uses the term *confidentiality* to refer to disclosure of information only to authorized individuals, entities, and so forth. *Privacy* refers to the social balance between an individual's right to keep information confidential and the societal benefit derived from sharing information, and how this balance is codified to give individuals the means to control personal information. The terms are not mutually exclusive: safeguards that help ensure confidentiality of information can be used to protect personal privacy.

information Safeguards and Security

OTA often uses the term *safeguard,* as in '(information safeguards" or '(to safeguard information." This is to avoid misunderstandings regarding use of the term "security," which some readers may interpret in terms of classified information, or as excluding measures to protect personal privacy. In discussion of information safeguards, the focus here is on technical and institutional measures to ensure the *confidentiality* and *integrity* of the information, and also the *authenticity* of its origin.

Cryptography can be used to fulfill these functions for electronic information. Modern *encryption* techniques, for example, can be used to safeguard the confidentiality of the contents of a message (or a stored file). *Integrity* is used to refer to the property that the information has not been subject to unauthorized or unexpected changes. *Authenticity* refers to the property that the message or information comes from the stated source or origin. *Message authentication* techniques and *digital signatures* 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).

SOURCE: Office of Technology Assessment, 1995. For more detailed discussion of cryptographic safeguards, see OTA, *Information Security and Privacy in Network Environments* (OTA-TCT-606, September 1994), esp. ch. 2 and 4 and appendix C.

sector and to federal-agency operations to safeguard unclassified information. As in the 1994 report, the focus is on safeguarding *unclassified* information. OTA's follow-on activities were conducted at the unclassified level and project staff did not receive or use any classified information during the course of this work.

Chapter 2 of this background paper gives an overview of the 1994 report. It highlights the importance of information security and privacy issues, explains why cryptography and cryptography policies are so important, and reviews policy findings and options from the 1994 report. Chapter 3 identifies major themes that emerged from a December 1994 OTA workshop, particularly regarding export controls and the international business environment, federal cryptography policy, and information-security "best practices." Chapter 4 provides an update on recent and ongoing cryptography, privacy, and security-policy developments and their relevance for possible congressional actions.

BOX 1-2: The 1994 OTA Re

In September 1994, the Office of Technology Assessment released its report *Information Security and Privacy in Network Environments.* In that report, OTA found that the fast-changing and competitive marketplace that produced the Internet and strong networking and software industries in the United States has not consistently produced products equipped with affordable, user-friendly safeguards. Many individual products and techniques are available to adequately safeguard specific information networks, if the user knows what to purchase, and can afford and correctly use the product, Nevertheless, better and more affordable products are needed. In particular, OTA found a need for products that *integrate* security features with other functions for use in electronic commerce, electronic mail, or other applications.

OTA found that more study is needed to fully understand vendors' responsibilities with respect to software and hardware product quality and liability. OTA also found that more study is also needed on the effects of export controls on the domestic and global markets for information safeguards, and on the ability of safeguard developers and vendors to produce more affordable, integrated products. OTA concluded that broader efforts to safeguard networked information will be frustrated unless cryptography-policy issues are resolved.

OTA found that the single most important step toward implementing proper safeguards for networked information in a federal agency or other organization is for top management to define the organization's overall objectives, define an organizational security policy to reflect those objectives, and implement that policy. Only top management can consolidate the consensus and apply the resources necessary to effectively protect networked information. For the federal government, this requires guidance from the Office of Management and Budget (e.g., in OMB Circular A-130), commitment from top agency management, and oversight by Congress.

During the course of the assessment (1993-94), there was widespread controversy concerning the Clinton Administration's escrowed-encryption initiative. The significance of this initiative, in concert with other federal cryptography policies, resulted in an increased focus in the report on the processes that the government uses to regulate cryptography and to develop federal information processing standards (the FIPS) based on cryptography.

The 1994 OTA report concluded that Congress has a vital role in formulating national cryptography policy and in determining how we safeguard information and protect personal privacy in an increasingly networked society (see the expanded discussion in appendix D of this background paper). Policy issues and options were identified in three areas: 1) cryptography policy, including federal information processing standards and export controls; 2) guidance on safeguarding unclassified information in federal agencies; and 3) legal issues and information security, including electronic commerce, privacy, and intellectual property.

SOURCE: Office of Technology Assessment, 1995; based on *Information Security and Privacy in Network Environments* (OTA-TCT-606, September 1994).

INFORMATION SECURITY AND PRIVACY IN A NETWORKED SOCIETY

Information technologies are transforming the ways in which we create, gather, process, and share information. Rapid growth in computer networking is driving many of these changes; electronic transactions and electronic records are becoming central to everything from business to health care. Within the federal government, effective use of information technologies and networks is central to government restructuring and reform.

The transformation being brought about by networking brings with it new concerns for the security of networked information and for our ability to maintain effective privacy protections in networked environments. Unless these concerns can

be resolved, they threaten to limit networking's full potential in terms of both participation and usefulness. Therefore, information safeguards (countermeasures) are achieving new prominence. Appropriate safeguards for the networked environment must account for—and anticipate—technical, institutional, and social changes that increasingly shift responsibility for security to the end users.

Computing power used to be isolated in large mainframe computers located in special facilities; computer system administration was centralized and carried out by specialists. In today's networked environment, computing power is decentralized to diverse users who operate desktop computers and who may have access to computing power and data at remote locations. Distributed computing and open systems can make every user essentially an "insider." In such a decentralized environment, responsibility for safeguarding information is distributed to the users, rather than remaining the purview of system specialists. The increase in the number and variety of network service providers also requires that users take responsibility for safeguarding information, rather than relying on intermediaries to provide adequate protection.[6]

The new focus is on safeguarding the *information* itself as it is processed, stored, and transmitted. This contrasts with older, more static or insulated concepts of "document" security or "computer" security. In the networked environment, we need appropriate rules for handling proprietary, copyrighted, and personal information—and tools with which to implement them.[7] Increased interactivity means that we must also deal with transactional privacy, as well as prevent fraud in electronic commerce and ensure that safeguards are integrated as organizations streamline their operations and modernize their information systems.

Importance of Cryptography

Cryptography (see box 2-1 on page 46) is not arcane anymore. It is a technology whose time has come—in the marketplace and in society. In its modern setting, cryptography has become a fundamental technology with broad applications.

Modern, computer-based cryptography began in the World War II era.[8] Much of this development has been shrouded in secrecy; in the United States, governmental cryptographic research has historically been the purview of the "national security" (i.e., defense and intelligence) communities. Despite two decades of growth in nongovernmental research and development, in the United States, the federal government still has the most expertise in cryptography. Nevertheless, cryptography is not just a "government technology" anymore, either.

Because it is a technology of broad application, the effects of federal policies about cryptography are not limited to technological developments in the field, 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.

Encryption (see box 2-2 on page 48) transforms a message or data files into a form that is unintelli-

[6] The trend is toward decentralized, distributed computing, rather than centralized, mainframe computing. Distributed computing is relatively informal and "bottom up," compared with mainframe computing, and systems administration may be less rigorous. See OTA, op. cit., footnote 5, pp. 3-5, 25-32.

[7] See ibid., chapter 3. "Security" technologies like encryption can be used to help protect privacy and the confidentiality of proprietary information; some, like digital signatures, could be used to facilitate copyright-management systems.

[8] See, e.g., David Kahn, *The Codebreakers* (New York, NY: MacMillan, 1967).

gible without special knowledge of some secret information (called the "decryption key").[9] Encryption can be used as a tool to protect the confidentiality of information in messages or files—hence, to help protect personal privacy. Other applications of cryptography can be used to protect the *integrity* of information (that it has not been subject to unauthorized or unexpected changes) and to *authenticate* its origin (that it comes from the stated source or origin and is not a forgery).

Thus, cryptography is a technology that will help speed the way to electronic commerce. With the advent of what are called *public-key* techniques, cryptography came into use for *digital signatures* (see figure 2-3 on page 52) 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 for ensuring that unauthorized changes or errors are detected (see discussion of message authentication and digital signatures in box 2-2).[10] These functions are critical for electronic commerce. Cryptographic techniques like digital signatures can also be used to help manage copyrighted material in electronic form.[11]

The nongovernmental markets for cryptography-based safeguards have grown over the past two decades, but are still developing. Good commercial encryption technology is available in the United States and abroad. Research in cryptography is international. Markets for cryptography also would be international, except for governmental restrictions (i.e., export controls), that effectively create "domestic" and "export" market segments for strong encryption products (see section on export controls below and also appendix C.[12] User-friendly cryptographic safeguards that are integrated into products (as opposed to those that the user has to acquire separately and add on) are still hard to come by—in part, because of export controls and other federal policies that seek to control cryptography.[13]

Cryptography and related federal policies (e.g., regarding export controls and standards development) were a major focus of the 1994 OTA report.[14] That focus was due in part from the widespread attention being given the so-called Clipper chip and the *escrowed-encryption* initiative announced by the Clinton Administration in 1993. Escrowed encryption, or *key-escrow encryption*, refers to an encryption method where the functional equivalent of a "spare key" must be deposited with a third party. The rationale for key-escrow encryption is to ensure government access to decryption keys when encrypted messages are encountered in the course of lawful electronic surveillance (see box 2-3 on page 54). The Escrowed Encryption Standard (EES), promulgated as a fed-

[9] Figures 2-1 and 2-2 on pages 50 and 51 illustrate two common forms of encryption: secret-key (or symmetric) encryption and public-key (or asymmetric) encryption. Note that key management—the generation of encryption and decryption keys, as well as their storage, distribution, cataloging, and eventual destruction—is crucial for the overall security of any encryption system.

[10] OTA, op. cit., footnote 5, pp. 69-77. See Peter H. Lewis, "Accord Is Reached on a Common Security System for the Internet," *The New York* Times, Apr. 11, 1995, p. D5.

[11] OTA, ibid., pp. 96-110. For example, digital signatures can be used to create compact "copyright tokens" for use in registries; encryption could be used to create personalized "copyright envelopes" for direct electronic delivery of material to customers. See also Working Group on Intellectual Property Rights, IITF, "Intellectual Property and the National Information Infrastructure (Green Paper)," July 1994, pp. 139-140.

[12] OTA, ibid., pp. 11-13, 150-160.

[13] Ibid., pp. 115-123, 128-132, 154-160.

[14] Ibid., pp. 8-18 and chapter 4.

eral information processing standard (FIPS) in 1994, is intended for use in encrypting unclassified voice, fax, or data communicated in a telephone system.[15] At present, all the Clipper chip (i.e., EES) "spare keys" are held within the executive branch.

Government Efforts To Control Cryptography

In its activities as a developer, user, and regulator of safeguard technologies, the federal government faces a fundamental tension between two policy objectives, each of which is important: 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. Cryptography is at the heart of this tension. Export controls and the federal standards process (i.e., the development and promulgation of federal information processing standards, or FIPS) are two mechanisms the government can use to control cryptography.[16]

Policy debate over cryptography used to be as arcane as the technology itself. Even 5 or 10 years ago, few people saw a link between government decisions about cryptography and their daily lives. However, as the information and communications technologies used in daily life have changed, concern over the implications of policies traditionally dominated by national security objectives has grown dramatically.

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 over other countries and preventing encryption devices from falling into the "wrong hands" overseas. More widespread foreign use—including use of strong encryption by terrorists and developing countries—makes U.S. signals intelligence more difficult.

Now, with an increasing policy focus on domestic crime and terrorism, the availability and use of cryptography has also come into prominence as a domestic-security, law enforcement issue.[17] Within the United States, strong encryption is increasingly 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:

> . . . Powerful encryption threatens to make worthless the access assured by the new digital law [i.e., the Communications Assistance for Law Enforcement Act].[18]

Thus, export controls, intended to restrict the international availability of U.S. cryptography technology and products, are now being joined with domestic cryptography initiatives, like key-escrow encryption, that are intended to preserve U.S. law enforcement and signals-intelligence capabilities.

Standards-development and export-control issues underlie a long history of concern over lead-

---

[15] The EES is implemented in hardware containing the Clipper chip. The EES (FIPS-185) specifies use of a classified, symmetric encryption algorithm, called *Skipjack*, which was developed by the National Security Agency. The Capstone chip implements the Skipjack algorithm for use in computer network applications. The Defense Department's FORTEZZA card (a PCMCIA card formerly called *TESSERA*) contains the Capstone chip.

[16] For more detail, see OTA, op. cit., footnote 5, chapters 1 and 4 and appendix C. Other means of control have historically included national security classification and patent-secrecy orders (see ibid., p. 128 and footnote 33).

[17] There is also growing organizational recognition of potentials for misuse of encryption, such as by disgruntled employees as a means to sabotage an employer's databases. Thus, some "commercial key-escrow" or "data recovery" facilities are being developed in the private sector (see discussion below and in ch. 4).

[18] Louis J. Freeh, Director, Federal Bureau of Investigation, testimony before the U.S. Senate, Committee on the Judiciary, Feb. 14, 1995, p. 27.

ership and responsibility (i.e., *"who should be in charge?"* and *"who is in charge?"*) for the security of unclassified information government-wide.[19] Most recently, these concerns have been revitalized by proposals presented by the Clinton Administration's Security Policy Board staff[20] to centralize information-security authorities under joint control of the Office of Management and Budget (OMB) and Defense Department (see discussion below and in chapter 4).

Other manifestations of these concerns can be found in the history of the Computer Security Act of 1987 (see below and appendix B) and in more recent developments, such as public reactions to the Clinton Administration's key-escrow encryption initiative and the controversial issuances of the Escrowed Encryption Standard[21] and Digital Signature Standard (DSS)[22] as federal information processing standards. Another important manifestation of these concerns is the controversy over the present U.S. export control regime, which includes commercial products with capabilities for strong encryption, including mass-market software, on the Munitions List, under State Department controls (see below and appendix C).

Federal Information Processing Standards

The 1994 OTA report concluded that two recent *federal information processing standards* based on cryptography are part of a long-term control strategy intended to retard the general, uncontrolled availability of strong encryption within the United States, for reasons of national security and law enforcement.[23] OTA viewed the Escrowed Encryption Standard and the Digital Signature Standard as complements in this overall control strategy, intended to discourage future development and use of encryption without built-in law enforcement access, in favor of key-escrowed encryption and related encryption technologies. If the EES and/or other key-escrow encryption standards (e.g., for use in computer networks) become widely used (or, at least, enjoy a large, guaranteed government market), this could ultimately reduce the variety of alternative cryptography products through market dominance that makes alternatives more scarce or more costly.

The Escrowed Encryption Standard is a federal information processing standard that uses a classified algorithm, called "Skipjack," developed by the National Security Agency (NSA). It was promulgated as a *voluntary* federal information processing standard. The Commerce Department's announcement of the EES noted that the standard does not mandate the use of escrowed-encryption devices by government agencies or the private sector; rather, the standard provides a mechanism for agencies to use key-escrow encryption without having to waive the requirements of another, extant federal encryption standard for unclassified information, the Data Encryption Standard (DES).[24]

The secret encryption/decryption key for Skipjack is 80 bits long. A key-escrowing scheme is built in to ensure "lawfully authorized" electronic surveillance.[25] The algorithm is classified and is

---

[19] OTA, op. cit., footnote 5, pp. 8-20 and chapter 4.

[20] U.S. Security Policy Board Staff, "Creating a New Order in U.S. Security Policy," Nov. 21, 1994, pp. II-III, 14-18.

[21] See box 2-3 in chapter 2 of this background paper and OTA, op. cit., footnote 5, chapter 4.

[22] See box 2-2 in chapter 2 of this background paper and OTA, ibid., appendix C.

[23] See OTA, op. cit., footnote 5, chapter 4.

[24] See *Federal Register*, vol. 59, Feb. 9, 1994, pp. 5997-6005 ("Approval of Federal Information Processing Standards Publication 185, Escrowed Encryption Standard (EES)"), especially p. 5998. Note however, that the DES is approved for encryption of unclassified data communications and files, while the EES is only a standard for telephone communications at this time.

[25] *Federal Register*, op. cit., footnote 22, p. 6003.

intended to be implemented only in tamper-resistant, hardware modules.[26] This approach makes the confidentiality function of the Skipjack encryption algorithm available in a controlled fashion, without disclosing the algorithm's design principles or thereby increasing users' abilities to employ cryptographic principles. One of the reasons stated for specifying a classified, rather than published, encryption algorithm in the EES is to prevent independent implementation of Skipjack without the law enforcement access features.

The EES is intended for use in encrypting unclassified voice, fax, and computer information communicated over a telephone system. The Skipjack algorithm can also be implemented for data encryption in computer networks; the Defense Department is using it in the Defense Message System. At this writing, however, there is no FIPS specifying use of Skipjack as a standard algorithm for data communications or file encryption. Given that the Skipjack algorithm was selected as a standard for telephony, it is possible that an implementation of Skipjack (or some other form of key-escrow encryption) will be selected as a FIPS to replace the DES for computer communications and/or file encryption. An alternative successor to the DES that is favored by nongovernmental users and experts is a variant of DES called *triple-encryption DES*. There is, however, no FIPS for triple-encryption DES.

Unlike the Skipjack algorithm, the algorithm in the federal Digital Signature Standard has been published.[27] 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 2-2). However, the DSS technique was chosen so that public-key encryption functions would *not* be available to users.[28] This is significant because public-key encryption is extremely useful for key management and could, therefore, contribute to the spread and use of nonescrowed encryption.[29] While other means of exchanging electronic keys are possible,[30] none is so mature as public-key technology. In contrast to the technique chosen for the DSS, the technique used in the most popular commercial digital signature system (based on the Rivest-Shamir-Adleman, or RSA, 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. At present, there is no FIPS for key exchange.

Federal Standards and the Computer Security Act of 1987

The Computer Security Act of 1987 (Public Law 100-235) is fundamental to development of federal standards for safeguarding unclassified information, to balancing national security and other objectives in implementing security and privacy policies within the federal government, and to other issues concerning government control of cryptography. Implementation of the Computer Security Act has been controversial, especially regarding the respective roles of the National Institute of Standards and Technology (NIST) and

[26] *Federal Register*, ibid., pp. 5997-6005.

[27] See appendix C of OTA, op. cit., footnote 5, for a history of the DSS.

[28] 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 that 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.)

[29] Public-key encryption can be used for confidentiality and, thereby, for secure key exchange. Thus, public-key encryption can facilitate the use of symmetric encryption methods like the DES or triple DES. See figure 2-3.

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

NSA in standards development and the chronic shortage of resources for NIST's computer security program to fulfill its responsibilities under the act (see detailed discussion in chapter 4 of the 1994 OTA report).[31]

The Computer Security Act of 1987 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 unclassified, sensitive information in federal government computer systems and would develop standards and guidelines to facilitate such protection. The act also established a Computer System Security and Privacy Advisory Board (CSSPAB). The board, appointed by the Secretary of Commerce, is charged with identifying emerging safeguard issues relative to computer systems security and privacy, advising the former National Bureau of Standards (now NIST) and the Secretary of Commerce on security and privacy issues pertaining to federal computer systems. The CSSPAB reports its findings to the Secretary of Commerce, the Director of OMB, the Director of NSA, and to the "appropriate committees of the Congress." Additionally, the act required federal agencies to identify computer systems containing sensitive information, to develop security plans for identified systems, and to provide periodic training in computer security for all federal employees and contractors who manage, use, or operate federal computer systems. Appendix B, drawn from the 1994 OTA report, provides more background on the purpose and implementation of the Computer Security Act and on the FIPS.

The Computer Security Act assigned responsibility for developing government-wide, computer-system security standards (e.g., the FIPS) and security guidelines and security-training programs to the National Bureau of Standards. According to its responsibilities under the act, NIST recommends federal information processing standards and guidelines to the Secretary of Commerce for approval (and promulgation, if approved). These FIPS do not apply to classified or "Warner Amendment" systems.[32] NIST can draw on the technical expertise of the National Security Agency in carrying out its responsibilities, but NSA's role according to the Computer Security Act, is an advisory, rather than leadership, one.

Federal Standards and the Marketplace

As the 1994 OTA report noted, not all government attempts at influencing the marketplace through the FIPS and procurement polices are successful. However, the FIPS usually do 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

[31] OTA, op. cit., footnote 5 and chapter 4 and appendix B. NIST's FY 1995 computer-security budget was on the order of $6.5 million, with $4.5 million of this coming from appropriated funds for "core" activities and the remainder from "reimbursable" funds from other agencies, mainly the Defense Department.

[32] The Warner Amendment (Public Law 97-86) excluded certain types of military and intelligence "automatic data processing equipment" procurements from the requirements of section 111 of the Federal Property and Administrative Services Act of 1949 (40 U.S.C. 795). Public Law 100-235 pertains to federal computer systems that come under section 111 of the Federal Property and Administrative Services Act of 1949.

technology like cryptography) and in convincing potential customers of product quality. 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.

In the 1970s, promulgation of the Data Encryption Standard as a stable and certified technology—at a time when the commercial market for cryptography-based safeguards for unclassified information was just 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 and international standards, in large part because it was a published standard that could be freely evaluated and implemented. The process by which the DES was developed and evaluated also stimulated private sector interest in cryptographic research, ultimately increasing the variety of commercial safeguard technologies. Although domestic products implementing the DES are subject to U.S. export controls, DES-based technology is available overseas.

The 1994 OTA report regarded the introduction of an incompatible *new* federal standard—for example, the Escrowed Encryption Standard—as destabilizing. At present, the EES and other implementations of Skipjack (e.g., for data communications) have gained little favor in the private sector. Features such as the government key-escrow agencies, classified algorithm, and hardware-only implementation all contribute to the lack of appeal. But, if key-escrow encryption technologies ultimately do manage to gain wide appeal in the marketplace, they might be able to "crowd out" safeguards that are based upon other cryptographic techniques and/or do not support key escrowing.[33]

The 1994 OTA report noted that this type of market distortion, intended to stem the supply of alternative products, may be a long-term objective of the key-escrow encryption initiative. 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. The costs of additional uncertainties and delays due to control interventions are ultimately borne by the private sector and the public.

Other government policies can also raise costs, delay adoption, or reduce variety. For example, export controls have the effect of segmenting domestic and export encryption markets. This creates additional disincentives to invest in the development—or use—of robust, but nonexportable, products with integrated strong encryption (see discussion below).

Export Controls

Another locus of concern is export controls on cryptography.[34] 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 (see appendix C). These regimes are administered by the State Department and the Commerce Department, respectively. Both regimes 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 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 under Commerce jurisdiction, no specific approval is required and a

[33] OTA, op. cit., footnote 5, pp. 128-132. A large, stable, lucrative federal market could divert vendors from producing alternative, riskier products; product availability could draw private sector customers.

[34] For more detail, see ibid. and chapters 1 and 4.

"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.[35]

Software and hardware for robust, user-controlled encryption are under State Department control, unless State grants jurisdiction to Commerce. This has become increasingly controversial, especially for the information technology and software industries.[36] 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 and thus have urgent need for sophisticated safeguards that can be used in operations worldwide, as well as for secure communications with overseas business partners, suppliers, and customers.[37] Software producers assert that, although other countries do have export and/or import controls on cryptography, several countries have more relaxed export controls on cryptography than does the United States.[38]

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 public explanation regarding the degree of success of these export controls and the necessity for maintaining strict controls on strong encryption in the face of foreign supply[39] and networks like the Internet that seamlessly cross national boundaries.[40]

Appendix C of this background paper, drawn from the 1994 OTA report, provides more background on export controls on cryptography. In September 1994, after the OTA report had gone to press, the State Department announced an amendment to the regulations implementing section 38 of the Arms Export Control Act. The new rule im-

---

[35] Ibid., pp. 150-154.

[36] To ease some of these burdens, the State Department announced new licensing procedures on Feb. 4, 1994. These changes were expected to include to include license reform measures for expedited distribution (to reduce the need to obtain individual licenses for each end user), rapid review of export license applications, personal-use exemptions for U.S. citizens temporarily taking encryption products abroad for their own use, and special licensing arrangements allowing export of key-escrow encryption products (e.g., EES products) to most end users. At this writing, expedited-distribution reforms were in place (*Federal Register*, Sept. 2, 1994, pp. 45621-45623), but personal-use exemptions were still under contention (Karen Hopkinson, Office of Defense Trade Controls, personal communication, Mar. 8, 1995).

[37] 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 Congress, 2d sess., Apr. 29 and May 7, 1992, Serial No. 65 (Washington, DC: U.S. Government Printing Office, 1992). See also discussion of business needs and export controls in chapter 3 of this background paper.

[38] OTA, op. cit., footnote 5, pp. 154-160. Some other countries do have stringent export and/or import restrictions.

[39] For example, the Software Publishers Association has studied the worldwide availability of encryption products and, as of October 1994, found 170 software products (72 foreign, 98 U.S.-made) and 237 hardware products (85 foreign, 152 U.S.-made) implementing the DES algorithm for encryption. (Trusted Information Systems, Inc. and Software Publishers Association, *Encryption Products Database Statistics*, October 1994.) Also see OTA, op. cit., footnote 5, pp. 156-160.

[40] For a discussion of export controls and network dissemination of encryption technology, see Simson Garfinkle, *PGP: Pretty Good Privacy* (Sebastopol, CA; O'Reilly and Assoc., 1995). PGP is an encryption program developed by Phil Zimmerman. Variants of the PGP software (some of which are said to infringe the RSA patent in the United States) have spread worldwide over the Internet. Zimmerman has been under grand jury investigation since 1993 for allegedly breaking the munitions export-control laws by permitting the software to be placed on an Internet-accessible bulletin board in the United States in 1991. (See Vic Sussman, "Lost in Kafka Territory," *U.S. News and World Report*, Apr. 3, 1995, pp. 30-31.)

plements one of the reforms applicable to encryption products that were announced on February 4, 1994, by the State Department.[41] Other announced reforms, still to be implemented, include special licensing procedures allowing export of key-escrow encryption products to "most end users."[42] The ability to export strong, key-escrow encryption products would presumably increase escrowed-encryption products' appeal to private-sector safeguard developers and users.

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 of 1994 (H.R. 3937), the House 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. In its report, the House 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 150 days 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.[43]

At the end of the 103d Congress, omnibus export administration legislation had not been enacted. Both the House and Senate bills contained language calling for the Clinton Administration to conduct comprehensive studies on the international market and availability of encryption technologies and the economic effects of U.S. export controls. In a July 20, 1994, letter to Representative Cantwell, Vice President Gore had assured her that the "best available resources of the federal government" would be used in conducting these studies and that the Clinton Administration would "reassess our existing export controls based on the results of these studies."[44]

At this writing, the Commerce Department and NSA are assessing the economic impact of U.S. export controls on cryptography on the U.S. computer software industry.[45] As part of the study, NSA is determining the foreign availability of encryption products. The study is scheduled to be delivered to the National Security Council by July 1, 1995. According to the National Security Council (NSC), it is anticipated that there will be both classified and an unclassified sections of the study; there may be some public release of the unclassified material.[46] In addition, an ongoing National Research Council (NRC) study that would support a broad congressional review of cryptography (and that is expected to address export controls) is due to be completed in 1996.[47] At this

---

[41] Department of State, Bureau of Political-Military Affairs, 22 CFR parts 123 and 124, *Federal Register*, vol. 59, No. 170, Sept. 2, 1994, pp. 45621-45623. See note 36 above and also ch. 4 of the 1994 OTA report. The reform established a new licensing procedure to permit U.S. encryption manufacturers to make multiple shipments of some encryption items directly to end users in approved countries, without obtaining individual licenses (see appendix C).

[42] Martha Harris, Deputy Assistant Secretary for Political-Military Affairs, U.S. Department of State, "Encryption—Export Control Reform," statement, Feb. 4, 1994. See OTA, op. cit., footnote 5, pp. 159-160.

[43] A study of this type (see below) is expected to be completed in mid-1995.

[44] Vice President Al Gore, letter to Representative Maria Cantwell, July 20, 1994. See OTA, op. cit., footnote 5, pp. 11-13.

[45] Maurice Cook, Bureau of Export Administration, Department of Commerce, personal communication, Mar. 7, 1995.

[46] Bill Clements, National Security Council, personal communication, Mar. 21, 1995.

[47] For information about the NRC study, which was mandated by Public Law 103-160, contact Herb Lin, National Research Council, 2101 Constitution Avenue, NW, Washington, DC 20418 (crypto@nas.edu). See discussion in OTA, op. cit., footnote 5, chapters 1 and 4.

writing, the NRC study committee is gathering public input on cryptography issues.

In the 104th Congress, Representative Toby Roth has introduced the "Export Administration Act of 1995" (H.R. 361). This bill did not include any specific references to cryptography. At this writing, it is not clear whether or when the contentious issue of cryptography export controls will become part of legislative deliberations.

Alternatively, the Clinton Administration could ease export controls on cryptography without legislation. As was noted above, being able to export key-escrow encryption products would presumably make escrowed-encryption products more attractive to commercial developers and users. Therefore, the Clinton Administration could ease export requirements for products with integrated key escrowing as an incentive for the commercial development and adoption of such products (see discussion of cryptography initiatives below and in chapter 4).

OTA WORKSHOP FINDINGS

At the request of the Senate Committee on Governmental Affairs, OTA held a workshop titled "Information Security and Privacy in Network Environments: What Next?" on December 6, 1994 as part of its follow-on activities after the release of the 1994 report. Workshop participants came from the business, legal, university, and public-interest communities. One workshop objective was to gauge participants' overall reactions to the OTA report *Information Security and Privacy in Network Environments.* Another was to identify related topics that merited attention and that OTA had not already addressed (e.g., network reliability and survivability or "corporate" privacy—see chapter 3). A third objective was for participants to identifyas specifically as possibleareas ripe for congressional action.

The general areas of interest were:

1. the marketplace for information safeguards and factors affecting supply and demand;
2. information-security "best practices" in the private sector, including training and implementation, and their applicability to government information security;
3. the impacts of federal information-security and policies on business and the public; and
4. desirable congressional actions and suggested time frames for any such actions.

Chapter 3 of this background paper highlights major points and opinions expressed by the workshop participants. It is important to note that the presentation in chapter 3 and the summary below are not intended to represent conclusions reached by the participants; moreover, the reader should not infer any general consensus, unless consensus is specifically noted.

Several major themes emerged from the discussion regarding export controls and the business environment, federal cryptography policy, and characteristics of information-security "best practices" that are germane to consideration of government information security. These have particular significance, especially in the context of current developments, for congressional consideration of several of the information-security issues and options identified in the 1994 OTA report. These themes include:

> *The mismatch between the domestic and international effects of current U.S. export controls on cryptography and the needs of business and user communities in an international economy.*

The need for reform of export controls was the number one topic at the workshop and perhaps the only area of universal agreement. Participants expressed great concern that the current controls are impeding companies' implementation of good security in worldwide operations and harming U.S. firms' competitiveness in the international marketplace. More than one participant considered that what is really at stake is loss of U.S. leadership in the information technology industry. As one participant put it, the current system is "a market intervention by the government with unintended bad consequences for both government and the private sector."

Several participants asserted that U.S. export controls have failed at preventing the spread of cryptography, because DES- and RSA-based encryption, among others, are available outside of this country. These considered that the only "success" of the controls has been to prevent major U.S. software companies from incorporating high-quality, easy-to-use, integrated cryptography in their products.

The intense dissatisfaction on the part of the private sector with the lack of openness and progress in resolving cryptography-policy issues.

Participants expressed frustration with the lack of a timely, open, and productive dialogue between government and the private sector on cryptography issues and the lack of response by government to what dialogue has taken place.[48] Many stressed the need for a genuine, open dialogue between government and business, with recognition that business vitality is a legitimate objective. Participants noted the need for Congress to broaden the policy debate about cryptography, with more public visibility and more priority given to business needs and economic concerns. In the export control arena, Congress was seen as having an important role in getting government and the private sector to converge on some feasible middle ground (legislation would not be required, if export regulations were changed). Leadership and timeliness ("the problem won't wait") were viewed as priorities, rather than more studies and delay.

Many felt the information-policy branches of the government are unable to respond adequately to the current leadership vacuum; therefore, they felt that government should either establish a more effective policy system and open a constructive dialogue with industry or leave the problem to industry.

The lack of public dialogue, visibility, and accountability, particularly demonstrated by the manner in which the Clipper chip was introduced and the EES promulgated, seemed to be a constant source of anger for both industry representatives and public interest groups. There were many concerns and frustrations about the role of the National Security Agency. Many participants suggested that this country desperately needs a new vision of "national security" that incorporates economic vitality. They consider that business strength is not part of NSA's notion of "national security," so it is not part of their mission. As one participant put it, "saying that 'we all have to be losers' on national security grounds is perverse industrial policy."

The mismatch between the federal standards process for cryptography-related FIPS and private sector needs for exportable, cost-effective safeguards.

As noted above, many participants viewed export controls as the single biggest obstacle to establishing international standards for information safeguards, One participant also noted the peculiarity of picking a national standard (e.g., a FIPS like the DES) and then trying to restrict its use internationally.

The question of the availability of secure products generated some disagreement over whether the market works or, at least, the extent to which it does and does not work. There was consensus that export controls and other government policies that segmented market demand were undesirable interventions. Though the federal government can use its purchasing power to significantly influence the market, most participants felt that this sort of market intervention would not be beneficial overall.

The mismatch between the intent of the Computer Security Act and its implementation.

There was widespread support for the Computer Security Act of 1987, but universal frustration with its implementation. NIST, the designated lead agency for security standards and guidelines, was described as underfunded and extremely

[48] See ibid., pp. 11-13, 150-160, 174-179.

slow. There was also a general recognition that people had been complaining about NIST for a while, but nothing has happened as a result of these complaints. Some participants noted the importance of increased oversight of the Computer Security Act of 1987 (Public Law 100-235), as well as possible redirection of NIST activities (e.g., collecting information about what industry is doing, pointing out commonalities and how to interoperate, rather than picking out a "standard").

According to some participants, the government should get "its house in order" in the civilian agencies and place more emphasis on unclassified information security. There was a perceived need for timely attention, because the architecture and policy constructs of the international information infrastructure are being developed right now, but these are "being left to the technologists" due to lack of leadership.

Several felt that the government has overemphasized cryptography, to the exclusion of management and problems like errors and dishonest employees that are not fully addressed by a "technology" focus. Participants considered that the real issue is *management*, not technology sloganism. According to participants, existing policies [e.g., the previous version of OMB Circular A-130, Appendix III] attempt to mandate cost-based models, but the implementation is ineffective. For example, after the Computer Security Act, NIST should have been in a position to help agencies, but this never happened due to lack of resources. Civil agencies lack resources, then choose to invest in new applications rather than spend on security. This is understandable when the observation that "nothing happens"—that is, no security incidents are detected—is an indicator of good security. Participants observed that, if inspectors general of government agencies are perceived as neither rewarding or punishing, users get mixed signals and conclude that there is a mismatch between security postures and management commitment to security implementation.

The distinction between security policies and guidelines for implementing these policies; and

the need for technological flexibility in implementing security policies.

Sound security policies are a foundation for good security practice. Importantly, these are not guidelines for implementation. Rather, they are "minimalist" directives that outline what must happen to maintain information security, but not how it must be achieved.

One of the most important things about these policies is that they are consistent across the entire company; regardless of the department, information-security policies are considered universally applicable. The policies have to be designed in a broad enough fashion to ensure that all company cultures will be able to comply. (Implementation of these polices can be tailored to fit specific needs and business practices.) Broad policy outlines allow information to flow freely between company divisions without increased security risk.

The workshop discussion noted the importance of auditing security implementation against policy, not against implementation guidelines. Good security policies must be *technology neutral*, so that technology upgrades and different equipment in different divisions would not affect implementation. Ensuring that policies are technology neutral helps prevent confusing implementation techniques and tools (e.g., use of a particular type of encryption or use of a computer operating system with a certain rating) with policy objectives, and discourages "passive risk acceptance" like mandating use of a particular technology. This also allows for flexibility and customization.

Workshop participants noted that, although the state of practice in setting security policy often has not lived up to the ideals discussed above, many companies are improving. At this point there are several road blocks frustrating more robust security for information and information systems. A primary road block is cost. Many systems are not built with security in mind, so the responsibility falls on the end user and retrofitting a system with security can be prohibitively expensive.

The need for line-management accountability for, and commitment to, good security, as opposed to "handing off" security to technology (i.e., hoping that a "technological fix" will be a cure-all).

The workshop discussion emphasized active risk acceptance by management and sound security policies as key elements of good information-security practice in the private sector. The concept of management responsibility and accountability as integral components of information security, rather than just "handing off" security to technology, were noted as very important by several participants. There was general agreement that direct support by top management and upper-management accountability are central to successful implementation of security policies. Many participants considered it vital that the managers understand active risk acceptance and not be insulated from risk.

Most security managers participating in the workshop viewed training as vital to any successful information-security policy. Lack of training leads to simple errors potentially capable of defeating any good security systemfor example, employees who write their passwords on paper and tape it to their computers. Several participants knew of companies that have fallen into the technology trap and have designed excellent computer security systems without sufficiently emphasizing training. There is a core of training material that is technology neutral and ubiquitous across the company. The necessity for impressing upon employees their role in information security was seen as paramount.

ISSUE UPDATE

Chapter 4 provides an update on executive-branch and private sector cryptography developments, business perspectives on government policies, congressional consideration of privacy issues, and government-wide guidance on information security in the federal agencies. The last section of chapter 4 discusses the implications of these developments for congressional consideration of some of the issues and options identified in the 1994 OTA report.

Government Cryptography Activities

In mid-1994, the executive branch indicated an openness toward exploring alternative forms of key-escrow encryption (i.e., techniques not implementing the Skipjack algorithm specified in the Escrowed Encryption Standard (EES) for use in computer and video networks.[49] However, there has been no formal commitment to eventually adopting any alternative to Skipjack in an escrowed-encryption FIPS for computer data.[50] Moreover, there has been no commitment to consider alternatives to the EES for telephony.

Furthermore, there has been no backing away from the underlying Clinton Administration commitment to "escrowing" encryption keys. With tightly integrated, or "bound" escrowing, there is mandatory key deposit. In the future, there may be some choice of escrow agencies or registries, but at present, Clipper- and Capstone-chip keys are being escrowed within the Commerce and Treasury Departments.[51] The Clinton Administration has not indicated an openness toward optional de-

[49] For background, see appendix D of this background paper and OTA, op. cit., footnote 5, pp. 15-16, 171-174. The Escrowed Encryption Standard is described in box 2-3 of this paper.

[50] See box 2-3. The Capstone chip refers to a hardware implementation of the EES's Skipjack algorithm, but for data communications. FORTEZZA (formerly TESSERA) is a PCMCIA card implementing Skipjack for data encryption, as well as the Digital Signature Standard (see box 2-2) and key-exchange functions.

[51] These chips implement the Skipjack algorithm for the EES and FORTEZZA applications, respectively.

posit of keys with registries, which OTA referred as "trusteeship" in the 1994 report (to distinguish it from the Clinton Administration's concept of key escrowing being required as an integral part of escrowed-encryption systems).[52]

The questions of whether or when there will be key-escrow encryption federal information processing standards for unclassified data communications and/or file encryption is still open. There is at present no FIPS specifying use of Skipjack for these applications. Implementation of key escrowing or trusteeship for large databases (i.e., encryption for file storage, as opposed to communications) has not been addressed by the government. However, commercial key depositories or data-recovery centers are being proposed by several companies (see next section on private sector developments).

Turning from encryption to digital signatures, acceptance and use of the new FIPS for digital signatures is progressing, but slowly. As the 1994 report detailed in its description of the evolution of the Digital Signature Standard, patent problems complicated the development and promulgation of the standard.[53] Patent-infringement uncertainties remain for the DSS, despite the government's insistence that the DSS algorithm does not infringe any valid patents and its offer to indemnify vendors that develop certificate authorities for a public-key infrastructure.[54]

Plans to implement the DSS throughout government are complicated by the relatively broad private sector use of a commercial alternative, the RSA signature system, and some agencies' desire to use the RSA system instead of, or alongside, the DSS. Cost, as well as interoperability with the private sector, is an issue. The DSS can be implemented in hardware, software, or firmware, but NSA's preferred implementation is in the "FORTEZZA" card.

The FORTEZZA card (formerly called the TESSERA card) is a Personal Computer Memory Card Industry Association (PCMCIA) card.[55] The FORTEZZA card is used for data communications; it implements the Skipjack algorithm, as well as key-exchange and digital-signature functions. FORTEZZA applications include the Defense Departments' Defense Message System. Per-workstation costs are significantly higher for the FORTEZZA card than for a software-based signature implementation alone. To use FORTEZZA, agencies must have—or upgrade to—computers with PCMCIA card slots, or must buy PCMCIA readers (about $125 each).

According to NSA, current full costs for FORTEZZA cards are about $150 each in relatively small initial production lots; of this cost, about $98 is for the Capstone chip. About 3,000 FORTEZZA cards had been produced as of April 1995 and another 33,000 were on contract. NSA hopes to award a large-scale production contract in fall 1995 for 200,000 to 400,000 units. In these quantities, according to the agency, unit costs should be

---

[52] See OTA, op. cit., footnote 5, p. 171.

[53] See OTA, op. cit., footnote 1, appendix C, especially pp. 220-221. For a more recent account of the various lawsuits and countersuits among patent holders, licensers, and licensees, see Simson Garfinkle, *PGP: Pretty Good Privacy* (Sebastopol, CA: O'Reilly and Assoc., 1995), esp. ch. 6.

[54] F. Lynn McNulty et al., NIST, "Digital Signature Standard Update," Oct. 11, 1994. The government offered to include an "authorization and consent" clause under which the government would assume liability for any patent infringement resulting from performance of a contract, including use of the DSS algorithm or public-key certificates by private parties when communicating with the government. See also OTA, op. cit., footnote 5, chapter 3.

[55] PCMCIA cards are slightly larger than a credit card, with a connector on one end that plugs directly into a standard slot in a computer (or reader). They contain microprocessor chips; for example, the FORTEZZA card contains a Capstone chip.

below the $100 per unit target established for the program.[56] Thus, the FORTEZZA production contract would be on the order of $20 million to $40 million.

NIST is working on what is intended to become a market-driven validation system for vendors' DSS products. This is being done within the framework of overall requirements developed for FIPS 140-1, "Security Requirements for Cryptographic Modules" (January 11, 1994). NIST is also developing a draft FIPS for "Cryptographic Service Calls" that would use relatively high-level application program interfaces (e.g., "sign" or "verify") to call on any of a variety of cryptographic modules. The intention is to allow flexibility of implementation in what NIST recognizes is a "hybrid world." Unfortunately, this work appears to have been slowed due to the traditional scarcity of funds for such core security programs at NIST (see chapter 2 and the 1994 OTA report, pages 20 and 164).

The 1996 Clinton Administration budget proposals reportedly do not specify funds for NIST work related to the DSS, or the EES.[57] However, according to the draft charter of the Government Information Technology Services Public-Key Infrastructure Federal Steering Committee, NIST will chair and provide administrative support for the Public-Key Infrastructure Federal Steering Commmittee that is being formed to provide guidance and assistance in developing an interoperable, secure public-key infrastructure to support electronic commerce, electronic mail, and other applications.

The Advanced Research Projects Agency (ARPA), the Defense Information Systems Agency (DISA), and NSA have agreed to establish an Information Systems Security Research Joint Technology Office (JTO) to coordinate research programs and long range strategic planning for information systems security research and to expedite delivery of security technologies to DISA. Part of the functions of the JTO will be to:

- Encourage the U.S. industrial base to develop commercial products with built-in security to be used in DOD systems. Develop alliances with industry to raise the level of security in all U.S. systems. Bring together private sector leaders in information security to advise the JTO and build consensus for the resulting program.
- Identify areas for which standards need to be developed for information systems security.
- Facilitate the availability and use of NSA certified cryptography within information systems security research programs.[58]

According to the Memorandum of Agreement establishing JTO, its work is intended to improve DISA's ability to safeguard the confidentiality, integrity, authenticity, and availability of data in Defense Department information systems, provide a "robust first line of defense" for defensive information warfare, and permit electronic com-

---

[56] Bob Drake, Legislative Affairs Office, NSA, personal communication, Apr. 7, 1995. To make the apparent price of FORTEZZA cards more attractive to Defense Department customers in the short term, NSA is splitting the cost of the Capstone chip with them, so agencies can acquire the early versions of FORTEZZA for $98 apiece (ibid.).

[57] Kevin Power, "Fate of Federal DSS in Doubt," *Government Computer News*, Mar. 6, 1995. The President's budget does provide $100 million to implement the digital wiretap legislation enacted at the close of the 103d Congress. See U.S. Congress, Office of Technology Assessment, *Electronic Surveillance in Advanced Telecommunications Networks—Background Paper,* forthcoming, spring 1995.

[58] "Memorandum of Agreement Between the Advanced Research Projects Agency, the Defense Information Systems Agency, and the National Security Agency Concerning the Information Systems Security Research Joint Technology Office," Mar. 3, 1995 (effective Apr. 2, 1995).

merce between the Defense Department and its contractors. (See discussion of the Defense Department's "Information Warfare" activities later in this chapter.)

Private Sector Cryptography Developments[59]

At the end of January 1995, AT&T Corp. and VLSI Technology, Inc., announced plans to develop an encryption microchip that would rival the Clipper and Capstone chips. The AT&T/VLSI chip will have the stronger, triple-DES implementation of the Data Encryption Standard algorithm.[60] It is intended for use in a variety of consumer devices, including cellular telephones, television decoder boxes for video-on-demand services, and personal computers.[61] The AT&T/VLSI chips do not include key escrowing. Under current export regulations, they would be subject to State Department export controls.

Industry observers consider this development especially significant as an indicator of the lack of market support for Clipper and Capstone chips because AT&T manufactures a commercial product using Clipper chips (the AT&T Surity Telephone Device) and VLSI is the NSA contractor making the chips that Mykotronx programs (e.g., with the Skipjack algorithm and keys) to become Clipper and Capstone chips.

The international banking and financial communities have long used encryption and authentication methods based on the DES. Because these communities have a large installed base of DES technology; a transition to an incompatible (non-DES-based) new technology would be lengthy. The Accredited Standards Committee X9, which sets data security standards for the U.S. banking and financial services industries, reportedly announced that it will develop new encryption standards based on triple DES and will designate a subcommittee to develop technical standards for triple-DES applications.[62]

RSA Data Security, Inc., recently announced another symmetric encryption algorithm, called RC5.[63] According to the company, RC5 is faster than the DES algorithm, is suitable for hardware or software implementation, and has a range of user-selected security levels. Users can select key lengths ranging up to 2,040 bits, depending on the levels of security and speed needed. The RSA digital signature system (see box 2-2 on page 48), from the same company, is the leading commercial rival to the Digital Signature Standard. RSA-based technology is also part of a new, proposed industry standard for protecting business transactions on the Internet.[64]

Another private sector standards group, the IEEE P1363 working group on public-key cryp-

---

[59] This section highlights selected government and commercial cryptography developments since publication of the 1994 OTA report. This is not a coomprehensive survey of commercial information-security products and proposals. Mention of individual companies or products is for illustrative purposes and/or identification only, and should not be interpreted as endorsement of these products or approaches.

[60] In "triple DES," the DES algorithm is used sequentially with three different keys, to encrypt, decrypt, then re-encrypt. Triple encryption with the DES offers more security than having a secret key that is twice as long as the 56-bit key specified in the FIPS. There is, however, no FIPS specifying triple DES.

[61] Jared Sandberg and Don Clark, "AT&T, VLSI Technology To Develop Microchips That Offer Data Security," *The Wall Street Journal*, Jan. 31, 1995; see also Brad Bass, op. cit., footnote 19.

[62] *CIPHER* (Newsletter of the IEEE Computer Society's TC on Security and Privacy), Electronic Issue No. 4, Carl Landwehr (ed.), Mar. 10, 1995, available from (http://www.itd.nrl.navy.mil/ITD/5540/ieee/cipher/cipher-archive.html).

[63] Ronald L. Rivest, "The RC5 Encryption Algorithm," *Dr. Dobb's Journal*, January 1995, pp. 146, 148.

[64] Peter H. Lewis, "Accord Is Reached on a Common Security System for the Internet," *The New York Times*, Apr. 11, 1995, p. D5. The proposed standard will be used to safeguard World Wide Web services.

tography, is developing a voluntary standard for "RSA, Diffie-Hellman, and Related Public-Key Cryptography" (see figure 2-5 on page 59). The group held a public meeting in Oakland, California, in May 1995 to review a draft standard.[65]

Several companies have proposed alternative approaches to key-escrow encryption; these include some 20 different alternatives.[66] Variously, these use published, unclassified encryption algorithms, thus potentially allowing software, as well as hardware, implementations. The commercial approaches would make use of commercial or private key-escrow systems, with data recovery services that are available to individuals and organizations, as well as to authorized law enforcement agencies.

A brief description of two of the commercial approaches is given in chapter 4, based on information provided by Trusted Information Systems (TIS) and Bankers Trust. The Bankers Trust system is hardware-based; the TIS system is software-based. Bankers Trust has proposed its system to the U.S. government and business community. The TIS system is under internal government review to determine the sufficiency of the approach to meet national security and law enforcement objectives.

Business Perspectives

Representatives of major U.S. computer and software companies have recently reaffirmed the importance of security and privacy protections in the developing *global* information infrastructure (GII).[67] But, as the Computer Systems Policy Project's "Perspectives on the Global Information Infrastructure" notes, there are strong and serious business concerns that government interests, especially in the standards arena, could stifle commercial development and use of networks in the international arena.

In June 1994, the Association for Computing Machinery (ACM) issued a report on the policy issues raised by introduction of the EES. The ACM report identified some key questions that need to be considered in reaching conclusions regarding:

> What cryptography policy best accommodates our national needs for secure communications and privacy, industry success, effective law enforcement, and national security?[68]

The U.S. Public Policy Committee of the ACM (USACM) issued a companion set of recommendations, focusing on the need for:

- open forums for cryptography policy development, in which government, industry, and the public could participate;
- encryption standards that do not place U.S. manufacturers at a disadvantage in the global marketplace and do not adversely affect technological development within the United States;
- changes in FIPS development, such as placing the process under the Administrative Procedures Act;
- withdrawal of the Clipper chip proposal by the Clinton Administration and the beginning of an open and public review of encryption policy; and
- development of technologies and institutional practices that will provide real privacy for fu-

---

[65] Ibid. Draft sections are available via anonymous ftp to rsa.com in the "pub/p1363" directory. The working group's electronic mailing list is <p1363@rsa.com>; to join, send e-mail to <p1363-request@rsa.com>.

[66] See Dorothy E. Denning and Dennis Branstad, "A Taxonomy for Key Escrow Encryption," forthcoming, obtained from the author (denning@cs.georgetown.edu); and Elizabeth Corcoran, "Three Ways To Catch a Code," *Washington Post*, Mar. 16, 1995, pp. B1, B12. The Corcoran article also discusses the Hewlett-Packard Co.'s proposed "national flag card" approach to government-approved encryption.

[67] See Computer Systems Policy Project, *Perspectives on the Global Information Infrastructure*, (Washington, DC: February 1995).

[68] Susan Landau et al., *Codes, Keys, and Conflicts: Issues in U.S. Crypto Policy* (New York, NY: Association for Computing Machinery, Inc., June 1994).

ture users of the National Information Infrastructure.[69]

Also in 1994, the International Chamber of Commerce (ICC) issued its "ICC Position Paper on International Encryption Policy." ICC noted 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 as "artificial obstacles" to trade. ICC urged governments "not to adopt a restrictive approach which would place a particularly onerous burden on business and society as a whole."[70] ICC's position paper called 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 recommended that global encryption policy be based on broad principles centered on openness and flexibility.[71]

The United States Council for International Business (USCIB) subsequently issued position papers on "Business Requirements for Encryption"[72] and "Liability Issues and the U.S. Administration's Encryption Initiatives."[73] The USCIB favored breaking down the "artificial barriers" to U.S. companies' competitiveness and ability to implement powerful security imposed by overly restrictive export controls. The Council called for international agreement on "realistic" encryption requirements, including: free choice of encryption algorithms and key management methods, public scrutiny of proposed standard algorithms, free export/import of accepted standards, and flexibility in implementation (i.e., hardware or software). If key escrowing is to be used, the USCIB proposed that:

- a government not be the sole holder of the entire key except at the discretion of the user;
- the key-escrow agent make keys available to lawfully authorized entities when presented with proper, written legal authorizations (including international cooperation when the key is requested by a foreign government);
- the process for obtaining and using keys for wiretapping purposes must be auditable;
- keys obtained from escrowing agents by law enforcement must be used only for a specified, limited time frame; and
- the owner of the key must (also) be able to obtain the keys from the escrow agent.[74]

The USCIB has also identified a number of distinctive business concerns regarding the U.S. government's position on encryption and liability:

- uncertainty regarding whether the Clinton Administration might authorize strict government liability for misappropriation of keys, including adoption of tamper proof measures to account for every escrowed unit key and family key (see box 2-3);
- the degree of care underlying design of Skipjack, EES, and Capstone (given the government's still-unresolved degree, if any, of liability);
- the confusion concerning whether the government intends to disclaim all liability in connec-

---

[69] U.S. Public Policy Committee of the ACM, "USACM Position on the Escrowed Encryption Standard," June 1994.

[70] International Chamber of Commerce, "ICC Position Paper on International Encryption Policy," Paris, 1994, pp. 2,3. See also United States Council for International Business, *Private Sector Leadership: Policy Foundations for a National Information Infrastructure (NII)*, July 1994, p 5.

[71] Ibid., pp. 3-4. See also chapter 4 of the 1994 OTA report.

[72] United States Council for International Business, "Business Requirements for Encryption," Oct. 10, 1994.

[73] United States Council for International Business, "Liability Issues and the U.S. Administration's Encryption Initiatives," Nov. 2, 1994.

[74] USCIB, op. cit., footnote 72, pp. 3-4.

tion with the EES and Capstone initiatives, and the extent to which family keys, unit keys, and law enforcement decryption devices will be adequately secured; and
- uncertainties regarding the liability of nongovernmental parties (e.g., chip manufacturers, vendors, and their employees) for misconduct or negligence.[75]

These types of concerns have remained unresolved (see related discussion and options presented in the 1994 OTA report, pages 16-18 and 171-182).

Liability issues are important to the development of electronic commerce and the underpinning institutional infrastructures, including (but not limited to) escrow agents for key-escrowed encryption systems and certificate authorities for public-key infrastructures. Widespread use of certificate-based, public-key infrastructures will require resolution and harmonization of liability requirements for trusted entities, whether these be federal certificate authorities, private certificate (or "certification") authorities, escrow agents, banks, clearinghouses, value-added networks, or other entities.[76]

There is increasing momentum toward frameworks within which to resolve legal issues pertaining to digital signatures and to liability. For example:

- The Science and Technology Section of the American Bar Association's Information Security Committee is drafting "Global Digital Signature Guidelines" and model digital-signature legislation.
- With participation by the International Chamber of Commerce and the U.S. State Department, the United Nations Commission on International Trade Law has completed a Model Law on electronic data interchange (EDI).
- Utah has just enacted digital signature legislation.[77]

Privacy Legislation

In the 104th Congress, bills have been introduced to address the privacy-related issues of search and seizure, access to personal records, content of electronic information, drug testing, and immigration and social security card fraud problems. In addition, Representative Cardiss Collins has reintroduced the "Individual Privacy Protection Act of 1995" (H.R. 184). H.R. 184 includes provisions to establish a Privacy Protection Commission charged with ensuring the privacy rights of U.S. citizens, providing advisory guidance on matters related to electronic data storage, and promoting and encouraging the adoption of fair information practices and the principle of collection limitation..

Immigration concerns and worker eligibility are prompting reexamination of social security card fraud and discussion over a national identification database. At least eight bills have been introduced in the 104th Congress to develop tamper-proof or counterfeit-resistant social security cards (H.R. 560, H.R. 570, H.R. 756, H.R. 785) and to promote research toward a national identification database (H.R. 502, H.R. 195, S. 456, S. 269).

Four bills have been introduced modifying search and seizure limitations: H.R. 3, H.R. 666, S. 3, and S. 54. The "Exclusionary Rule Reform Act of 1995" (H.R. 666 and companion S. 54), which revises the limitations on evidence found during a search, passed the House on February 10,

---

[75] USCIB, op. cit., footnote 73, pp. 2-6.

[76] See ibid. for discussion of liability exposure, legal considerations, tort and contract remedies, government consent to be liable, and recommendations and approaches to mitigate liability.

[77] Information on American Bar Association and United Nations activities provided by Michael Baum, Principal, Independent Monitoring, personal communication, Mar. 19, 1995. See also Michael S. Baum, *Federal Certification Authority Liability and Policy: Law and Policy of Certificate-Based Public Key and Digital Signatures*, NIST-GCR-94-654, NTIS Doc. No. PB94-191-202 (Springfield, VA: National Technical Information Service, 1994).

1995. Similar provisions have been included in crime legislation introduced in both houses, S. 3 and H.R. 3. The Senate Committee on the Judiciary has held a hearing on Title V of S. 3, the provisions reforming the exclusionary rule.

Also this session, legislation has been introduced increasing privacy protection by restricting the use or sale of lists collected by communication carriers (H.R. 411) and the U.S. Postal Service (H.R. 434), defining personal medical privacy rights (H.R. 435, S. 7), detailing acceptable usage of credit report information (H.R. 561), and mandating procedures for determining the reliability of drug testing (H.R. 153). These bills establish guidelines in specific areas, but do not attempt to address the overall challenges facing privacy rights in an electronic age.

The "Family Privacy Bill" (H.R. 1271) passed the House on April 4, 1995. H.R. 1271, introduced by Representative Steve Horn on March 21, 1995, is intended to provide parents the right to supervise and choose their children's participation in any federally funded survey or questionnaire that involves intrusive questioning on sensitive issues.[78] Some have raised concerns about the bill on the grounds that it might dangerously limit local police authority to question minors and threaten investigations of child abuse, or hinder doctors in obtaining timely patient information on children.[79]

In addition, the Office of Management and Budget recently published notice of draft privacy principles and draft security tenets for the national information infrastructure.[80] The draft privacy principles were developed by the Information Infrastructure Task Force's Working group on Privacy and are intended to update and revise the Code of Fair Information Practices developed in the early 1970s and used in development of the Privacy Act of 1974.

Information-Security Policy Initiatives and Legislation

The Defense Department's "Information Warfare" activities address the opportunities and vulnerabilities inherent in its (and the country's) increasing reliance on information and information systems. The Department has a variety of Information Warfare activities ongoing in its services and agencies, the Office of the Secretary of Defense, and elsewhere.[81] The Department's Defensive Information Warfare program goals focus on technology development to counter vulnerabilities stemming from the Department's growing dependence on information systems and the commercial information infrastructure (e.g., the public-switched network and the Internet). The Information Systems Security Research Joint Technology Office established by ARPA, DISA, and NSA (see above) will pursue research and development pursuant to these goals.

The increasing prominence of Information Warfare issues has contributed to an increasing momentum for consolidating information-security authorities government-wide, thereby expanding the role of the defense and intelligence agencies for unclassified information security overall:

> . . . Protection of U.S. information systems is also clouded by legal restrictions put forth, for example, in the Computer Security Act of 1987.

---

[78] Representative Scott McInnis, *Congressional Record*, Apr. 4, 1995, p. H4126.

[79] Representative Cardiss Collins, *Congressional Record*, Apr. 4, 1995, p. H4126.

[80] Office of Management and Budget, "National Information Infrastructure: Draft Principles for Providing and Using Personal Information and Commentary," *Federal Register*, vol. 60, No. 13, Jan. 20, 1995, pp. 4362-4370. These were developed by the Privacy Working Group of the Information Policy Committee, Information Infrastructure Task Force (IITF). See also Office of Management and Budget, "Draft Security Tenets for the National Information Infrastructure," *Federal Register*, vol. 60, No. 28, Feb. 10, 1995, p. 8100. These were developed by the Security Issues Forum of the IITF.

[81] See, e.g., "Report of the Defense Science Board Summer Study Task Force on Information Architecture for the Battlefield," Office of the Under Secretary of Defense for Acquisition and Technology, October 1994.

> Of concern to the Task Force is the fact that IW [Information Warfare] technologies and capabilities are largely being developed in an open commercial market and are outside of direct Government control.[82]

Such a consolidation and/or expansion would run counter to current statutory authorities and to OMB's proposed new government-wide security and privacy policy guidance (see below).

The Joint Security Commission

In mid-1993, the Joint Security Commission was convened by the Secretary of Defense and the Director of Central Intelligence to develop a "new approach to security that would assure the adequacy of protection within the contours of a security system that is simplified, more uniform, and more cost effective."[83] The Joint Security Commission's report made recommendations across a comprehensive range of areas.

The sections on information systems security[84] and a security architecture for the future[85] are of special interest. In the context of the Commission's charter, they propose a unified security policy structure and authority for classified and unclassified information in the defense/intelligence community.[86] However, the report also recommends a more general centralization of information security along these lines government-wide; the executive summary highlights the conclusion the security centralization within the defense/intelligence community described in the report should be extended government-wide.[87] The report also recommends "establishment of a national level security policy committee to provide structure and coherence to U.S. government security policy, practices, and procedures."[88]

The Security Policy Board

On September 16, 1994, President Clinton signed Presidential Decision Directive 29 (PDD-29). PDD-29, "Security Policy Coordination," established a new structure, under the direction of the National Security Council (NSC), for the coordination, formulation, evaluation, and oversight of U.S. security policy.[89] According to the description of PDD-29 provided to OTA by NSC, the directive designates the former Joint Security Executive Committee established by the Secretary of Defense and the Director of Central Intelligence as the *Security Policy Board*.

The Security Policy Board (SPB) subsumes the functions of a number of previous national security groups and committees. The SPB members include the Director of Central Intelligence, Deputy Secretary of Defense, Vice Chairman of the Joint Chiefs of Staff, Deputy Secretary of State, Under Secretary of Energy, Deputy Secretary of Commerce, and Deputy Attorney General; plus one Deputy Secretary from "another non-defense-related-agency" selected on a rotating basis, and one representative each from the OMB and NSC staff.

The Security Policy Forum that had been established under the Joint Security Executive Com-

---

[82] Ibid., p. 52.

[83] Joint Security Commission, "Redefining Security: A Report to the Secretary of Defense and Director of Central Intelligence," Feb. 28, 1994 (quote from letter of transmittal). See also U.S. Congress, House of Representatives, Permanent Select Committee on Intelligence, "Intelligence Authorization Act for Fiscal Year 1994," Rept. 103-162, Part I, 103d Congress, 1st session, June 29, 1993, pp. 26-27.

[84] Joint Security Commission, ibid., pp. 101-113.

[85] Ibid., pp. 127 et seq.

[86] Ibid., p. 105, first paragraph.; p. 110, recommendation; pp. 127-130.

[87] Ibid., p. viii, top.

[88] Ibid., p. 130.

[89] Although it is unclassified, PDD-29 has not been released. This discussion is based on a fact sheet provided to OTA by NSC; the fact sheet is said to be a "nearly verbatim text of the PDD," with the only differences being "minor grammatical ones." David S. Van Tassel (Director, Access Management, NSC), letter to Joan Winston (OTA), and enclosure, Feb. 16, 1995.

mittee was retained under the SPB. The forum is composed of senior representatives from over two dozen defense, intelligence, and civilian agencies and departments; the forum chair is appointed by the SPB chair. The Security Policy Forum functions are to: consider security policy issues raised by its members or others, develop security policy initiatives and obtain comments for the SPB from departments and agencies, evaluate the effectiveness of security policies, monitor and guide the implementation of security policies to ensure coherence and consistency, and oversee application of security policies to ensure they are equitable and consistent with national goals.[90]

PDD-29 also established a Security Policy Advisory Board of five members from industry. This independent, nongovernmental advisory board is intended to advise the President on implementation of the policy principles guiding the "new" formulation, evaluation, and oversight of U.S. security policy, and to provide the SPB and the intelligence community with a "public interest" perspective. The SPB is authorized to establish interagency working groups as necessary to carry out its functions and to ensure interagency input to and coordination of security policy, procedures, and practices, with staffs to support the SPB and any other groups or fora established pursuant to PDD-29.

PDD-29 was not intended to change or amend existing authorities or responsibilities of the members of the SPB, as "contained in the National Security Act of 1947, other existing laws or Executive Orders."[91] PDD-29 does not refer specifically to government *information* security policy, procedures, and practices, or to *unclassified* information security government-wide. Nevertheless, the proposed detailed implementation of the directive with respect to information security, as articulated in the Security Policy staff report report, "Creating a New Order in U.S. Security Policy," is a departure from the information security structure set forth in the Computer Security Act of 1987. The staff report appears to recognize this mismatch between its proposal and statutory authorities for unclassified information security, noting the Computer Security Act under information-security "actions required" to implement PDD-29.[92]

The SPB staff's proposed "new order" for information security builds on the Joint Security Commission's analysis and recommendations to establish a "unifying body" government-wide.[93] With respect to information security, the new SPB structure would involve organizing an Information Systems Security Committee (ISSC) charged with "coupling the development of policy for both the classified and the sensitive but unclassified communities" and a "transition effort" for conversion to the new structure.[94]

This "comprehensive structure" would be the new ISSC, that would be:

> . . . based on the foundation of the current NSTISSC [see appendix B of this background paper] but will have responsibility for both the classified and the sensitive but unclassified world.
>
> The ISSC would be jointly chaired at the SES [Senior Executive Service] or General Officer level by DOD and OMB. This new body would consist of voting representatives from each of the agencies/departments currently represented on the NSTISSC and its two subcommittees, NIST and the civil agencies it represents, and other appropriate agencies/departments, such as DISA, which are currently not represented on the NSTISSC. This

---

[90] Ibid. (fact sheet).

[91] Ibid.

[92] U.S. Security Policy Board Staff, "Creating a New Order in U.S. Security Policy," Nov. 21, 1994. p. 18.

[93] Ibid., p. 3. See Elizabeth Sikorovsky, "NSC Proposes To Shift Policy-Making Duties," *Federal Computer Week*, Jan. 23, 1995, pp. 1, 45. See also Kevin Power, "Administration Floats New Information Security Policy," *Government Computer News*, Jan. 23, 1995, p. 59.

[94] U.S. Security Policy Board Staff , op. cit., footnote 92, pp. II-III, p. 15.

body would create working groups as needed to address topics of interest.

The ISSC would eventually have authority over all classified and unclassified but sensitive systems, and would report to through the [Security Policy] Forum and Board to the NSC. Thus, policies would have the full force and authority of an NSC Directive, rather than the relatively "toothless" issuances currently emanating from the NSTISSC. NSA would continue to provide the secretariat to the new national INFOSEC structure, since the secretariat is a well-functioning, highly-efficient, and effective body.

. . . A joint strategy would have to be devised for a smooth transition between the current and new structures, which would ensure that current momentum is maintained and continuity preserved. *In addition, a new definition must be developed for "national security information," and it must be determined how such information relates to the unclasified arena from a national security standpoint* [emphasis added]. Issues such as voting in such a potentially unwieldy organization must also be resolved.[95]

At this writing, the extent to which the SPB information-security proposals, ISSC, and the development of a new definition of "national security information" have or have not been "endorsed" within the executive branch is unclear. Outside the executive branch, however, they have been met with concern and dismay reminiscent of reactions to NSDD-145 a decade ago (see chapter 2 and appendix B).[96] Moreover, they run counter to the statutory agency authorities set forth in the 104th Congress in the Paperwork Reduction Act of 1995 (see below), as well as in the Computer Security Act of 1987. At its March 23-24, 1995 meeting, the Computer Systems Security and Privacy Board that was established by the Computer Security Act issued Resolution 95-3, recommending that the SPB await broader discussion of issues before proceeding with its plans "to control unclassified, but sensitive systems."

Concerns have also been expressed within the executive branch. The ISSC information security structure that would increase the role of the defense and intelligence communities in governmentwide unclassified information security runs counter to the Clinton Administration's "basic assumptions" about free information flow and public accessibility as articulated in the 1993 revision of OMB Circular A-130, "Management of Federal Information Resources."[97]

Moreover, some senior federal computer security managers have expressed concern about what they consider *premature implementation* of the SPB staff report's proposed centralization of information security functions and responsibilities. In a January 11, 1995, letter to Sally Katzen, Director of the Office of Information and Regulatory Affairs, Office of Management and Budget (released March 23, 1995), the Steering Committee of the Federal Computer Security Program Manager's Forum[98] indicated "unanimous disagreement" with the Security Policy Board's (SPB) proposal and urged OMB to "take appropriate action to restrict implementation of the SPB report to only classified systems."[99] This type of restriction appears to have been incorporated in the proposed revision to Appendix III of OMB Circular A-130 (see below).

---

[95] Ibid., pp. 17-18. See appendix B of this paper and OTA, op. cit., footnote 5, pp. 132-148 for discussion of NSDD-145, the intent of the Computer Security Act of 1987, and NSTISSC.

[96] See Neil Munro, "White House Security Panels Raise Hackles," *Washington Technology*, Feb. 23, 1995, pp. 6, 8.

[97] OMB Circular A-130—Revised, June 25, 1993, Transmittal Memorandum No. 1, sec. 7.

[98] The Federal Computer Security Program Manager's Forum is made up of senior computer security managers for civilian agencies, including the Departments of Commerce, Health and Human Services, Justice, and Transportation. The January 11, 1995, letter to Sally Katzen. Director of the Office of Information and Regulatory Affairs, Office of Management and Budget, was signed by Lynn McNulty, Forum Chair (National Institute of Standards and Technology) and Sadie Pitcher, Forum Co-chair (Department of Commerce). Text of letter taken from the online *EPIC Alert*, vol. 2.05, Mar. 27, 1995.

[99] Ibid.

In March and April 1995, OTA invited the Security Policy Board staff to comment on draft OTA text discussing information-security centralization, including the Joint Security Commission report, PDD-29, and the SPB staff report. OTA received SPB staff comments in early May 1995, as this background paper was in press. According to the Security Policy Board staff director, information systems security policy is a "work in progress in its early stages" for the SPB and the staff report was intended to be a "strawman" starting point for discussion. Moreover, according to the SPB staff, "recognizing the sensitivity and complexity of Information Systems Security policy, the ISSC was not one of the committees which was established, nor was a transition team formed."[100] In order to provide as much information as possible for consideration of information security issues, including the SPB staff perspective, OTA has included the SPB staff comments in box 1-3.

The Paperwork Reduction Act of 1995

The Paperwork Reduction Act was reauthorized in the 104th Congress. The House and Senate versions of the Paperwork Reduction Act of 1995 (H.R. 830 and S.244) both left existing agency authorities under the Computer Security Act of 1987 unchanged.[101] The Paperwork Reduction Act of 1995 (Public Law 104-13) was reported on April 3, 1995,[102] passed in both Houses on April 6, 1995, and signed by President Clinton on May 22, 1995.

Among its goals, the Paperwork Reduction Act of 1995 is intended to make federal agencies more responsible and publicly accountable for information management. With respect to safeguarding information, the act seeks to:

> . . . ensure that the creation, collection, maintenance, use, dissemination, and disposition of information by or for the Federal Government is consistent with applicable laws, including laws relating to—
>
> (A) privacy and confidentiality, including section 552a of Title 5;
> (B) security of information, including the Computer Security Act of 1987 (Public Law 100-235); and
> (C) access to information, including section 552 of Title 5.[103]

With respect to privacy and security, the Paperwork Reduction Act of 1995 provides that the Director of OMB shall:

1. develop and oversee the implementation of policies, principles, standards, and guidelines on privacy, confidentiality, security, disclosure, and sharing of information collected or maintained by or for agencies;
2. oversee and coordinate compliance with sections 552 and 552a of title 5, the Computer Security Act of 1987 (40 U.S.C. 759 note), and related information management laws; and
3. require Federal agencies, consistent with the Computer Security Act of 1987 (40 U.S.C. 59 note), to identify and afford security

---

[100] Peter D. Saderholm (Director, Security Policy Board Staff), memorandum for Joan D. Winston and Miles Ewing (OTA), SPB 095-95, May 4, 1995.

[101] Senator William V. Roth, Jr., *Congressional Record*, Mar. 6, 1995, p. S3512.

[102] U.S. Congress, House of Representatives, "Paperwork Reduction Act of 1995—Conference Report to Accompany S.244," H. Rpt. 104-99, Apr. 3, 1995. As the "Joint Explanatory Statement of the Committee of the Conference" (ibid., pp. 27-39) notes, the 1995 act retains the legislative history of the Paperwork Reduction Act of 1980. Furthermore, the definition of "information technology" in the 1995 act is intended to preserve the exemption for military and intelligence information technology that is found in current statutory definitions of "automatic data processing." The 1995 act accomplishes this by referring to the so-called Warner Amendment exemptions to the Brooks Act of 1965 and, thus, to section 111 of the Federal Property and Administrative Services Act (ibid., pp. 28-29). See also discussion of the Warner Amendment exemptions from the FIPS and the Computer Security Act in appendix B of this background paper.

[103] Ibid., sec. 3501(8). The act amends chapter 35 of title 44 U.S.C.

protections commensurate with the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of information collected or maintained by or on behalf of an agency.[104]

The latter requirement for cost-effective security implementation and standards is tied to the roles of the Director of NIST and the Administrator of General Services in helping the OMB to:

(A) develop and oversee the implementation of polices, principles, standards, and guidelines for information technology functions and activities of the Federal Government, including periodic evaluations of major information systems; and

(B) oversee the development and implementation of standards under section 111(d) of the Federal Property and Administrative Services Act of 1949 (40 U.S.C. 759(d)).[105]

Federal agency heads are responsible for ensuring that their agencies shall:

1. implement and enforce applicable policies, procedures, standards, and guidelines on privacy, confidentiality, security, disclosure, and sharing of information collected or maintained by or for the agency;
2. assume responsibility and accountability for compliance with and coordinated management of sections 552 and 552a of title 5, the Computer Security Act of 1987 (40 U.S.C. 759 note), and related information management laws; and
3. consistent with the Computer Security Act of 1987 (40 U.S.C. 59 note), identify and afford security protections commensurate with the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of information collected or maintained by or on behalf of an agency.[106]

Proposed Revision of Appendix III of OMB Circular A-130

At this writing, OMB had just completed the proposed revision of Appendix III. The proposed revision is intended to lead to improved federal information-security practices and to make fulfillment of Computer Security Act and Privacy Act requirements more effective generally, as well as with respect to data sharing and secondary uses. As indicated above, the Paperwork Reduction Act of 1995 has affirmed OMB's government-wide authorities for information security and privacy.

The new, proposed revision of Appendix III ("Security of Federal Automated Information") will be key to assessing the prospect for improved federal information security practices. The proposed revision was posted for public comment on March 29, 1995. According to OMB, the proposed new government-wide guidance:

> . . . is intended to guide agencies in securing information as they increasingly rely on an open and interconnected National Information Infrastructure. It stresses management controls such as individual responsibility, awareness and training, and accountability, rather than technical controls . . .
>
> The proposal would also better integrate security into program and mission goals, reduce the need for centralized reporting of paper security plans, emphasize the management of risk rather than its measurement, and revise government-wide security responsibilities to be consistent with the Computer Security Act.[107]

According to OMB, the proposed new security guidance reflects the significant differences in ca-

---

[104] Ibid., sec. 3504(g). The OMB Director delegates authority to administer these functions to the Administrator of OMB's Office of Information and Regulatory Affairs.

[105] Ibid., section 3504(h)(1). See also "Joint Explanatory Statement of the Committee of the Conference," ibid., pp. 27-29.

[106] Ibid., section 3506(g).

[107] Office of Management and Budget, "Security of Federal Automated Information," Proposed Revision of OMB Circular No. A-130 Appendix III (transmittal memorandum), available via World Wide Web at http://csrc.ncsl.nist.gov/secplcy as <a130app3.txt>.

BOX 1-3: Security Policy Board Staff Perspectives on Information-Security Issues

OTA note: This material presents Security Policy Board staff views on information security issues and the SPB staff report. It was excerpted from SPB staff comments to OTA and has been edited for length.

. . . [T]he general area of Information Systems Security presents us all with one of the most difficult and controversial aspects of security policy. Because of this, there has been a great deal of recent analysis and activity in the area of Information Systems Security policy involving the Security Policy Board (SPB), the Security Policy Forum (SPF), and out supporting Staff. Because of the fast pace of recent events, and the fact that for the SPB/SPF, Information Systems Security policy is a "work in progress" in its early stages, we have not done the best job in getting the word out to the community beyond the 26 agencies and departments that are represented in the SPB on the current status of our Information Systems Security-related activities. [The OTA background paper] may provide an excellent vehicle for presenting a balanced view of Executive Branch analysis and activity in this critical policy area.

. . . The [section above on information-security policy initiatives] begins by accurately noting that network security issues are of great concern, and then suggests that DOD activity under the name of "Information Warfare" (IW) is raising awareness of threats to networks, and is contributing to the momentum for consolidating Information Systems Security authorities government-wide, thereby increasing the role of the defense and intelligence agencies. While that may be true to some extent, the draft is silent on other reasons why there may be a "momentum" for at least considering the advisability of consolidating some aspects of government Information Systems Security policymaking, e.g., the increasing internetworking across the "classified' and "unclassified" communities. Others may argue that the splitting of Information Systems Security responsibilities by Public Law 100-235 simply isn't working to provide the level of systems security both communities need—failing for many of the same reasons the PDD-24 failed when it attempted to split Communications Security (COMSEC) authorities along similar lines. However, it is not the role of the SPB/SPF Staff to take a position on these issues, but rather to act as an "honest broker" within the Executive Branch to ensure that all aspects of security policy receive an informed, balanced review. In pursuing this role, we have recognized the relationship of defensive IW to Information Systems Security policy, but do not see it as the only, or even the primary, driver of whatever momentum exists to consolidate Executive Branch Information Systems Security responsibilities. Many of the issues surrounding the "consolidation" question-e. g., efficient use of limited government resources—have no trace of the Defense/Intelligence flavor of DOD Information Warfare activities. . .

[OTA'S description] of PDD-29 and its organization creations is mostly accurate although you err in implying that the structure is DOD and Intelligence Community oriented. Actually, quite the opposite is true. In fact, if OTA were to be challenged to develop a senior level government-wide board to serve as a "fair court" to adjudicate information systems security and other security policy issues, you would quite likely develop an entity very similar if not the same as the SPB. The majority of the SPB itself comes from the civil agencies. . . [T]he very important Security Policy Forum (SPF) includes among its 26 members the Departments of Commerce, Energy, Justice, State, Treasury, Transportation, and representatives from OMB, National Aeronautics and Space Administration, Nuclear Regulatory Commission, Office of Personnel Management, General Services Administration, and Federal Emergency Management Agency. Again, the majority of the SPF membership is from the civil agencies. Quite frankly, we find it ironic that your draft gives significant credence to negative comments about the SPB efforts credited to representatives of Commerce and the OMB when both the Deputy Secretary of Commerce and the Deputy Director of the OMB sit on the SPB and have been active participants in the SPB deliberations to date.

BOX 1-3 (cont'd.): Security Policy Board Staff Perspectives on Information-Security Issues

In PDD-29, the President observed, "We require a new security process based on sound threat analysis and risk management practices. A process which can adapt our security policies, practices and procedures as the economic, political and military challenges to our national interests continue to evolve." The President further charged the SPB to conduct a review of all of our nation's security policies, practices and procedures and make recommendations for needed change after such proposals have been coordinated with all US. departments and agencies affected by such decisions.

At the first SPB meeting on 27 September 1994, the SPB Staff was charged with starting a government-wide dialogue on the various elements of security policy by developing a "strawman" proposal. The Staff attempted to start this by publishing the "New Order" paper, which simply contained *proposals* [emphasis in original] for how the government might more effectively address the various security disciplines, as recommended by the Joint Security Commission (JSC). Many of the Staff recommendations were "no brainers. " In the field of personnel security, for example, the government had already consolidated its efforts into one entity. In essence, the SPB Staff attempted to begin the dialogue by suggesting the most simple structure possible to address government-wide security policy. The SPB and SPF subsequently acted on some of the report's proposals and established transition teams and committees for four of the six committees proposed in the report. A fifth will be established in mid-May. However, recognizing the sensitivity and complexity of Information Systems Security policy, the ISSC was not one of the committees which was established, nor was a transition team formed. Those who view the establishment of the other committees as somehow transforming the Staff Report into official administration policy are mistaken, and it is unfortunate that so many have chosen to misrepresent the Staff Report. I can assure you that the SPB, SPF, and Staff have not presented the "New Order" report as anything other than an early effort at establishing a starting point for serious dialogue on overall security policy.

The idea of an ISSC with government-side scope has, as fully expected, met with opposition from various parties for various reasons. It is our goal to facilitate an informed discussion of the information systems security issues facing our nation, and to have that informed discussion occur at the appropriate levels within the government. Our review to date has focused almost exclusively on the ever growing area where the classified community and the unclassified community intersect. Therein are any number of government owned systems which may be considered critical to the safety and security of our nation and its people: systems such as the Federal Election System, air traffic control and those that control our nation's power grid, for example. It has generally been assumed that the private sector, to the extent possible, will develop the needed security for these systems. This may be true, but the question remains that if an "Oklahoma City" like incident occurs in one or more of these systems, who will our nation, the Congress, and our President turn to. To that end, we framed the "scope" issue for the SPF, which, in turn, raised the issue at the 24 April 1995 meeting of the SPB. The outcome of that meeting was direction by the SPB to its member agencies to attempt development of Terms of Reference for an interagency group to study these issues and report back to the SPB. The SPB Staff has, therefore, scheduled a meeting to begin that process which [took] place on 4 May 1995. In keeping with our efforts to be the "honest broker," the Staff has invited all member agencies, Office of Science and Technology Policy and other interested departments and agencies representing the widely divergent points of view with regard to this subject.

(continued)

BOX 1-3 (cont'd.): Security Policy Board Staff Perspectives on Information-Security Issues

In taking this initiative, the Deputy Secretaries that comprise the SPB recognize that they may be subject to criticism. However, their concerns about taking positive action to avoid catastrophe in any number of these critical systems was best summed up when one observed, "Shame on us if we don't at least try!"

The SPB, SPF, and Staff have not and never will propose that any information systems security actions will be taken which are contrary to law, government regulations, or directives. It does not necessarily follow, however, that issues cannot be explored, that ideas cannot be considered, or that new approaches to difficult security problems cannot be explored which are outside the context of preexisting policies, laws, regulations, and organizational structures. It is entirely possible that what was appropriate in 1987 may not be completely adequate in 1995. Information technology has advanced manyfold since then; the National Information Infrastructure has developed and the information systems security challenges facing the classified and unclassified communities have become more similar, Indeed, the very reason for establishing the JSC was to develop *new* approaches to security that would "assure the adequacy of protection within the contours of a security system that is *simplified, more uniform, and more cost effective* [emphasis in original], As referenced earlier in PDD-29, the President directed that "The SPB will be the principal mechanism for reviewing and proposing to the NSC legislative initiatives and executive orders pertaining to U.S. security policy, procedures, and practices. . ." If an informed dialogue within the government, across the Executive and Legislative Branches, leads to a common sense view to make Information Systems Security policy in a manner different from the way it is currently done, then laws, policies, regulations, and organizational structures could certainly be adjusted to accomplish national Information Systems Security goals. Again, it is our role on the SPB/SPF Staff to facilitate that informed dialogue.

SOURCE. Excerpted from Peter D. Saderholm (Director, Security Policy Board Staff), memorandum to Joan D. Winston and Miles Ewing (OTA), May 4, 1995,

pabilities, risks, and vulnerabilities of the present computing environment, as opposed to the relatively closed, centralized processing environment of the past. Today's processing environment is characterized by open, widely distributed information-processing systems that are interconnected with other systems within and outside government and by an increasing dependence of federal agency operations on these systems. OMB's "federal information technology world" encompasses over 2 million individual workstations (e.g., PCs), but only some 25,000 medium and large computers.[108] Accordingly, a major focus of OMB's new guidance is on end users and decentralized information-processing systems—and the information-processing applications they use and support.

According to OMB, the proposed revision of Appendix III stresses management controls (such as individual responsibility, awareness, and training) and accountability, rather than technical controls. OMB also considers that the proposed security appendix would better integrate security into agencies' program and mission goals, reduce the need for centralized reporting of paper security plans, emphasize the management of risk rather than its measurement, and revise government-wide security responsibilities to be consistent with the Computer Security Act.[109]

[108] Ed Springer, OMB, personal communication, Mar. 23, 1995.

[109] Office of Management and Budget, op. cit., footnote 107.

OMB's proposed new security appendix:

> . . . proposes to re-orient the Federal computer security program to better respond to a rapidly changing technological environment. It establishes government-wide responsibilities for Federal computer security and requires Federal agencies to adopt a minimum set of management controls.
>
> These management controls are directed at individual information technology users in order to reflect the distributed nature of today's technology. For security to be most effective, the controls must be a part of day-to-day operations. This is best accomplished by planning for security not as a separate activity, but as part of overall planning.
>
> "Adequate security" is defined as "security commensurate with the risk and magnitude of harm from the loss, misuse, or unauthorized access to or modification of information." This definition explicitly emphasizes the risk-based policy for cost-effective security established by the Computer Security Act.[110]

The new guidance assigns the Security Policy Board responsibility for (only) "national security policy coordination in accordance with the appropriate Presidential directive [e.g., PDD 29]."[111] With respect to national security information:

> Where an agency processes information which is controlled for national security reasons pursuant to an Executive Order or statute, security measures required by appropriate directives should be included in agency systems. Those policies, procedures, and practices will be coordinated with the U.S. Security Policy Board as directed by the President.[112]

Otherwise, the proposed OMB guidance assigns government-wide responsibilities to agencies that is "consistent with the Computer Security Act." These agencies include the Department of Commerce, through NIST; the Department of Defense, through NSA; the Office of Personnel Management; the General Services Administration; and the Department of Justice.[113]

A complete analysis of the proposed revision to Appendix III is beyond the scope of this background paper. In brief, the proposed new guidance reflects a fundamental and necessary shift in emphasis from securing automated information *systems* to safeguarding automated *information* itself. It seeks to accomplish this through:

- controls for general support systems (including hardware, software, information, data, applications, and people) that share common functionality and are under the same direct management control; and
- controls for major applications (that require special attention due to their mission-critical nature).

For each type of control, OMB seeks to ensure managerial accountability by requiring management officials to *authorize in writing*, based on review of implementation of the relevant security plan, use of the system or application. For general support systems, OMB specifies that use should be re-authorized at least every three years. Similarly, major applications must be authorized before operating and reauthorized at least every three years thereafter. For major applications, management authorization implies accepting the risk of each system used by the application.[114]

This type of active risk acceptance and accountability, coupled with review and reporting requirements, is intended to result in agencies ensuring that adequate resources are devoted to implementing "adequate security." Every three years (or when significant modifications are made), agencies must review security controls in systems and major applications and correct deficiencies. Depending on the severity, agencies must also con-

---

[110] Ibid., p. 4.

[111] Ibid., p. 15.

[112] Ibid., pp. 3-4.

[113] Ibid., pp. 14-16.

[114] Ibid., pp. 2-6.

sider identifying a deficiency in controls pursuant to the Federal Manager's Financial Accountability Act. Agencies are required to include a summary of their system security plans and major application security plans in the five-year plan required by the Paperwork Reduction Act.

IMPLICATIONS FOR CONGRESSIONAL ACTION

Appendix D of this paper, based on chapter 1 of the 1994 OTA report on information security and privacy, reviews the set of policy options in that report. OTA identified policy options related to three general policy areas:

1. national cryptography policy, including federal information processing standards and export controls;
2. guidance on safeguarding unclassified information in federal agencies; and
3. legal issues and information security, including electronic commerce, privacy, and intellectual property.

In all, OTA identified about two dozen possible options. The need for openness, oversight, and public accountability—given the broad public and business impacts of these policies—runs throughout the discussion of possible congressional actions. During its follow-on work, OTA found that recent and ongoing events have relevance for congressional consideration of policy issues and options identified in the 1994 report, particularly in the first two areas noted above.

In OTA's view, two key questions underlying consideration of options addressing cryptography policy and unclassified information security within the federal government are:

1. How will we as a nation develop and maintain the balance among traditional "national security" (and law enforcement) objectives and other aspects of the public interest, such as economic vitality, civil liberties, and open government?
2. What are the costs of government efforts to control cryptography and who will bear them?

Some of these costs—for example, the incremental cost of requiring a "standard" solution that is less cost-effective than the "market" alternative in meeting applicable security requirements—may be relatively easy to quantify, compared with others. But none of these cost estimates will be easy to make. Some costs may be extremely difficult to quantify, or even to bound—for example, the impact of technological uncertainties, delays, and regulatory requirements on U.S. firms' abilities to compete effectively in the international marketplace for information technologies. Ultimately, however, these costs are all borne by the public, whether in the form of taxes, product prices, or foregone economic opportunities and earnings.

The remainder of this chapter discusses possible congressional actions related to cryptography policy and government information security, in the context of the policy issues and options OTA identified in the 1994 report. These options can be found in appendix D of this background paper and pp. 16-20 of the 1994 report. For the reader's convenience, the pertinent options are discussed in boxes 1-4 through 1-7 in this chapter.

Cryptography Policy and Export Controls

In the 1994 study and its follow-on work, OTA has observed that many of the persistent concerns surrounding the Clinton Administration's escrowed-encryption initiative focus on whether key-escrow encryption will become mandatory for government agencies or the private sector, if nonescrowed encryption will be banned, and/or if these actions could be taken without legislation. Other concerns still focus on whether or not alternative forms of encryption would be available that would allow private individuals and organizations the option of depositing keys (or not) with one or more third-party trustees—at their discretion (see pp. 8-10, 14-18, 171-182 of the 1994 OTA report).

Congressional Review of Cryptography Policy

OTA noted that an important outcome of a congressional review of national cryptography policy would be the development of more open processes to determine how cryptography will be deployed

BOX 1-4: Congressional Review of Cryptography Policy

OTA concluded that information to support a congressional policy review of cryptography is out of phase with implementation. Therefore, OTA noted that:

OPTION: Congress could consider placing a hold on further deployment of key-escrow encryption, pending a congressional policy review.

More open processes would build trust and confidence in government operations and leadership. More openness would 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 would also allow for public consensus-building, providing better information for use in congressional oversight of agency activities. Toward these ends, OTA noted that:

OPTION: Congress could address the extent to which the current working relationship between the National Institute of Standards and Technology and National Security Agency 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 of a broad policy review would be a clarification of national information-policy principles in the face of technological change:

OPTION: Congress could state its policy as to when the impacts of a technology (like cryptography) are so powerful and pervasive that legislation is needed to provide sufficient public visibility and accountability for government actions.

SOURCE: Office of Technology Assessment, 1995; based on *Information Security and Privacy in Network Environments* (OTA-TCT-606, September 1994).

throughout society, including development of the public-key infrastructures and certification authorities that will support electronic delivery of government services and digital commerce.

In 1993, Congress asked the National Research Council to conduct a major study that would support a broad review of cryptography and its deployment; the results are expected to be available in 1996. The NRC study should be valuable in helping Congress to understand the broad range of technical and institutional alternatives. However, if implementation of the EES and related technologies continues at the current pace, OTA has noted that key-escrow encryption may already be embedded in information systems before Congress can act on the NRC report.

Therefore, OTA's options for congressional consideration (see box 1-4) included an option to place a hold on further deployment of escrowed encryption within the government, pending a congressional review, as well as options addressing open policy implementation, and public visibility and accountability. These are still germane, especially given the NSA's expectation of a large-scale investment in FORTEZZA cards and the likelihood that nondefense agencies will be encouraged by NSA to join in adopting FORTEZZA.

There has been very little information from the Clinton Administration as to the current and projected costs of the escrowed-encryption initiative, including costs of the current escrow agencies for Clipper and Capstone chips and total expenditures anticipated for deployment of escrowed-encryption technologies. (NSA has indicated that a FORTEZZA procurement contract on the order of $20 million to $40 million may be awarded in fall 1995.)

Export Controls

Reform of the current export controls on cryptography was certainly the number one topic at the

BOX 1-5: Export Controls on Cryptography

As part of a broad national cryptography policy, OTA noted that 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 examination would take into account changes in foreign capabilities and foreign availability of cryptographic technologies.

Information from an executive branch study of the encryption market and export controls that was promised by Vice President Gore should provide some near-term information. The Department of Commerce and the National Security Agency (NSA) are assessing the economic impact of U.S. export controls on the U.S. computer software industry; as part of this study, NSA is determining the foreign availability of encryption products. The study is scheduled to be delivered to the National Security Council deputies by July 1, 1995.

OTA noted that the scope and methodology of the export-control studies that Congress might wish to use in the future may differ from those used in the executive-branch study. Therefore:

OPTION: Congress might wish to assess the validity and effectiveness of the Clinton Administration's studies of export controls on cryptography by conducting oversight hearings, by undertaking a staff analysis, or by requesting a study from the Congressional Budget Office.

SOURCE: Off Ice of Technology Assessment, 1995: based on *Information Security and Privacy in Network Environments* (OTA-TCT-606, September 1994).

December 1994 OTA workshop. More generally, the private sector's priority in this regard is indicated by the discussion of the industry statements of business needs above. Legislation would not be required to relax controls on cryptography, if this were done by revising the implementing regulations. However, the Clinton Administration has previously evidenced a disinclination to relax controls on robust cryptography, except perhaps for certain key-escrow encryption products.[115]

The Export Administration Act is to be reauthorized in the 104th Congress. The issue of export controls on cryptography may arise during consideration of export legislation, or if new export procedures for key-escrow encryption products are announced, and/or when the Clinton Administration's market study of cryptography and controls is completed this summer (see box 1-5).

Aside from any consideration of whether or not to include cryptography provisions in the 1995 export administration legislation, Congress could advance the convergence of government and private sector interests into some "feasible middle ground" through hearings, evaluation of the Clinton Administration's market study, and by encouraging a more timely, open, and productive dialogue between government and the private sector (see pages 11-13, 150-160, 174-179 of the 1994 OTA report.)

Responses to Escrowed Encryption Initiatives

The 1994 OTA report recognized that Congress has a near-term role to play in determining the extent to which—and how—the EES and other escrowed-encryption systems will be deployed in

[115] See appendix C of this backgroud paper, especially footnote 10 and accompanying text.

BOX 1-6: Congressional Responses to Escrowed-Encryption Initiatives

In responding to current escrowed-encryption initiatives like the Escrowed Encryption Standard (EES), and in determining the extent to which appropriated funds should be used in implementing key-escrow encryption and related technologies, OTA noted that:

OPTION: Congress could address 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.

With respect to current escrowed-encryption initiatives like the EES, as well as any subsequent key-escrow encryption initiatives (e.g., for data communications or file encryption), and in determining the extent to which appropriated funds should be used in implementing key-escrow encryption and related technologies, OTA noted that:

OPTION: Congress could address the issue of criminal penalties for misuse and unauthorized disclosure of escrowed key components.

OPTION: Congress could consider allowing damages to be awarded for individuals or organizations who were harmed by misuse or unauthorized disclosure of escrowed key components.

SOURCE: Office of Technology Assessment, 1995; based on *Information Security and Privacy in Network Environments* (OTA-TCT-606, September 1994).

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 Clinton Administration has stated that it has no plans to make escrowed encryption mandatory, or to ban other forms of encryption. But, absent legislation, these intentions are not binding for future administrations and also leave open the question of what will happen if the EES and related technologies do not prove acceptable to the private sector. Moreover, the executive branch may soon be using the EES and/or related escrowed-encryption technologies (e.g., FORTEZZA) to safeguard-among other things—large volumes of private and proprietary information.

For these reasons, OTA concluded that the EES and other key-escrowing initiatives are by no means only an executive branch concern. The EES and any subsequent escrowed-encryption standards (e.g., for data communications in computer networks, or for file encryption) 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. Therefore, OTA identified options addressing location of escrow agents, as well as criminal penalties and civil liabilities for misuse or unauthorized disclosure of escrowed key components (see box 1-6). These are still germane, and the liability issues are even more timely, given recent initiatives by the international legal community and the states.

Safeguarding Unclassified Information in the Federal Agencies

The need for congressional oversight of federal information security and privacy is even more urgent in a time of government reform and streamlining. When the role, size, and structure of the federal agencies are being reexamined, it is important to take into account the additional in-

formation security and privacy risks incurred in downsizing and the general lack of commitment on the part of top agency management to safeguarding unclassified information.

A major problem in the agencies has been lack of top management focus on, not to mention responsibility and accountability for, information security. As the 1994 OTA report noted:

> The single most important step toward implementing proper information safeguards for networked information in a federal agency or other organization is for top management to define the organization's overall objectives and a security policy to reflect those objectives. Only top management can consolidate the consensus and apply the resources necessary to effectively protect networked information. For the federal government, this means guidance from OMB, commitment from top agency management, and oversight by Congress. (p. 7)

All too often, agency managers have regarded information security as "expensive overhead" that could be skimped on, deferred, or foregone in favor of other expenditures (e.g., for new computer hardware and applications). Any lack of priority and resources for safeguarding information is increasingly problematic as we move toward increased secondary use of data, data sharing across agencies, and decentralization of information processing and databases. If this mindset were permitted to continue during agency downsizing and program consolidation, the potential—and realized—harms from "disasters waiting to happen" can be much greater. (See pages 1-8, 25-31, and 40-43 of the 1994 OTA report.) For example, without proper attention to information security, staffing changes during agency restructuring and downsizing can increase security risks (due to unstaffed or understaffed security functions, reductions in security training and implementation, large numbers of disgruntled former employees, etc.).

OTA's ongoing work has spotlighted important elements of good information-security practice in the private sector, including active risk acceptance by line management. The concept of management responsibility and accountability as integral components of information security, rather than just "handing off" security to technology, is very important.

Sound security policies as a foundation for practice are essential; these should be technology neutral. Technology-neutral policies specify what must be done, not how to do it. Because they do not prescribe implementations, technology-neutral policies are longer lived. They are not so easily obsoleted by changes in technology or business practices; they allow for local customization of implementations to meet operational requirements. Once these are in place, security implementation should be audited against policy, not against implementation guidelines. This helps prevent confusing implementation techniques and tools (e.g., use of a particular type of encryption or use of an computer operating system with a certain rating) with policy objectives, and discourages "passive risk acceptance" like mandating use of a particular technology. This also allows for flexibility and customization.

In the federal arena, however, more visible energy seems to have been focused on debates over implementation tools—that is, federal information processing standards like the Data Encryption Standard, Digital Signature Standard, and Escrowed Encryption Standard—than on formulating enduring, technology-neutral policy guidance for the agencies.

Direction of Revised OMB Guidance

In the 1994 report, OTA identified the need for the revised version of the security appendix (Appendix III) of OMB Circular A-130 to adequately address problems of managerial responsibility and accountability, insufficient resources devoted to information security, and overemphasis on technology, as opposed to management. In particular, OTA noted the importance of making agency line management (not just "information security officers") accountable for information security and ensuring that privacy and other policy objectives are met. Moreover, OTA noted that the proposed new OMB guidance would have to provide sufficient incentives—especially in times of budget

cuts—to ensure that agencies devote adequate resources to safeguarding information. Similarly, the OMB guidance would have to ensure that information safeguards are treated as an integral component when systems are designed or modified.

The proposed revision to Appendix III of OMB Circular A-130, as discussed above, shows promise for meeting these objectives. OMB's proposed guidance is intended to incorporate critical elements of the following: considering security as integral (rather than an add-on) to planning and operations, active risk acceptance, line management responsibility and accountability, and focus on management and people rather than technology. Taken as a whole, these elements are intended to provide sufficient incentives for agency managements to devote adequate resources to security; the review and reporting requirements offer disincentives for inadequate security. Moreover, if implemented properly, the new OMB approach can make significant progress in the ultimate goal of tracking and securing the information itself, as it is gathered, stored, processed, and shared among users and applications.

However, OMB's twofold approach is somewhat abstract and a significant departure from earlier, "computer security" guidance. Therefore, congressional review and oversight of OMB's proposed revisions to Appendix III, as suggested in the 1994 OTA report (see box 1-7), would be helpful in ensuring that Congress, as well as federal agencies and the public, understand the new information-security guidance and how OMB intends for its new approach to be implemented.

This congressional review and oversight might also provide additional guidance on how NIST's security activities might best be refocused to meet federal information-security objectives. For example, in addition to Commerce's (i.e., NIST's) traditional responsibilities for security standards and training and awareness, the new Appendix III assigns Commerce responsibilities for providing agencies with guidance and assistance concerning effective controls when systems are interconnected, coordinating incident response activities to promote information-sharing regarding incidents and related vulnerabilities, and (with Defense Department technical assistance) evaluating new information technologies to assess their security vulnerabilities and apprising agencies of these in a timely fashion.[116]

Locus of Authority

Another reason for the importance and timeliness of congressional oversight of governmentwide information-security policy guidance is that there is renewed momentum for extending the defense/intelligence community's centralization of information-security responsibilities throughout the civil agencies as well. If initiatives such as the Information Systems Security Committee structure presented in the Security Policy Board staff report come to fruition, information-security responsibilities for both the civilian agencies and the defense/intelligence agencies would be merged.

An overarching issue that must be resolved by Congress is where federal authority for safeguarding unclassified information in the civilian agencies should reside and, therefore, what needs to be done concerning the substance and implementation of the Computer Security Act of 1987. If Congress retains the general premise of the act—that responsibility for unclassified information security in the civilian agencies should not be placed within the defense/intelligence community—then vigilant oversight and clear direction will be needed to ensure effective implementation, including assigning and funding a credible focal point(s) for unclassified information security (see discussion of OMB Appendix III above and also pp. 19-20 of the 1994 OTA report).

Without doubt, leadership and expertise are needed for better, more consistent safeguarding of unclassified information government-wide. But it

[116] OMB, op. cit., footnote 82, p. 7.

BOX 1-7: Safeguarding Information in Federal Agencies

Congress has an even more direct role in establishing the policy guidance within which federal agencies safeguard information, and in oversight of agency and Office of Management and Budget measures to implement information security and privacy requirements. The new, proposed revision of Appendix Ill ("Security of Federal Automated Information") of OMB Circular A-130 is intended to lead to improved federal information-security practices and to make fulfillment of Computer Security Act and Privacy Act requirements more effective generally, as well as with respect to data sharing and secondary uses.

The options presented below are in the context of the 1994 report and the previous version of Appendix Ill. However, OTA expects that congressional oversight and analysis as indicated below will remain useful for understanding OMB's new guidance and assessing its potential effectiveness. OTA noted that, after the revised Appendix Ill of OMB Circular A-130 issued:

OPTION: Congress could 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, and/or requesting a study from the General Accounting Office. However, the effects of OMB's revised guidance may not be apparent for some time after the revised Appendix Ill 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:

OPTION: Congress could 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 that are developing major new information systems. in the course of its oversight and when considering the direction of any new legislation, OTA noted that:

OPTION: Congress could ensure that agencies include explicit *provisions for safeguarding information assets in any information-technology planning documents.*

is not clear that there are no workable alternatives to centralizing government-wide information-security responsibilities under the defense/intelligence community. Proposals to do so note current information-security deficiencies; however, many of these can be attributed to lack of commitment to and funding for establishment of an alternative source of expertise and technical guidance for the civilian agencies. For example, the "efficiency" arguments (see below) made in the Joint Security Commission report and the Security Policy Board staff report for extending the responsibilities of the defense/intelligence community to encompass government-wide security for classified and unclassified information capitalize on the vacuum in leadership and expertise created by chronic underfunding of the designated civilian agency—at present, NIST. (See pp. 13-16, 20, 138-150, and 182-183 of the OTA report.)

Proposals for centralizing security responsibilities for both classified and unclassified information government-wide offer efficiency arguments to the effect that:

1. security policies, practices, and procedures (as well as technologies) for unclassified information are for the most part spin-offs from the classified domain;
2. the defense and intelligence agencies are expert in classified information security; and therefore

BOX 1-7 (cont'd.): Safeguarding Information in Federal Agencies

OPTION: Congress could ensure that agencies budget sufficient resources to safeguard information assets, whether as a percentage of information-technology modernization and/or operating budgets, or otherwise.

OPTION: Congress could ensure that the Department of Commerce assigns sufficient resources to the National Institute of Standards and Technology to support its Computer Security Act responsibilities, as well as NET's other activities related to safeguarding information and protecting privacy in networks.

Regarding NIST's computer-security budget, OTA did not determined the extent to which additional funding is needed, or the extent to which additional funding would improve the overall effectiveness of NEST's information-security activities. Additional resources, whether from overall increases in NIST's budget or otherwise, could enhance NIST's technical capabilities, enable it to be more proactive, and hence be more useful to federal agencies and to industry. OTA found that NIST activities regarding 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, OTA concluded that national security constraints set forth in executive branch policy directives appear to be binding. These constraints have resulted, for example, in the closed processes by which the FIPS known as the Escrowed Encryption Standard (Clipper) was developed and implemented.

Increased funding could enable NIST to become a more equal partner to the National Security Agency, 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, OTA concluded that clear policy guidance and oversight (not just funding) will be needed.*

SOURCE" Office of Technology Assessment, 1995; based on *Information Security and Privacy in Network Environments* (OTA-TCT-606, September 1994).

3. the unclassified domain can best be served by extending the authority of the defense/intelligence agencies.

The validity of the "spin-off" assumption about unclassified information security is questionable. There are real questions about NSA's ability to place the right emphasis on cost-effectiveness, as opposed to absolute effectiveness, in flexibly determining the most appropriate means for safeguarding unclassified information. Due to its primary mission in securing classified information, NSA's traditional culture tends toward a standard of absolute effectiveness, not trading off cost and effectiveness. By contrast, the Computer Security Act of 1987, the Paperwork Reduction Act of 1995, and the new, proposed revision of OMB Appendix 111 all require agencies to identify and employ cost-effective safeguards, for example:

> With respect to privacy and security, the Director [of OMB] shall . . . require Federal agencies, consistent with the Computer Security Act of 1987 (940 U.S.C. 759 note) security protections commensurate with the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of information collected or maintained by or on behalf of an agency.[117]

[117] "Paperwork Reduction Act of 1995" (S. 244), section 3504(g)(3), Mar. *7, 1995, Federal Record,* p. S3557.

Moreover, the current state of government security practice for unclassified information has been depressed by the chronic shortage of resources for NIST's computer security activities in fulfillment of its government-wide responsibilities under the Computer Security Act of 1987. Since enactment of the Computer Security Act, there has been no serious (i.e., adequately funded and properly staffed), sustained effort to establish a center of information-security expertise and leadership outside the defense/intelligence communities.

Even if the efficiency argument is attractive, Congress would still need to consider whether the gains would be sufficient to overcome the concomitant decrease in "openness" in information-security policymaking and implementation, and/or whether the outcomes would fall at an acceptable point along the "efficiency-openness" possibility frontier. In the area of export controls on cryptography, for example, there is substantial public concern with the current tradeoff between the needs of the defense/intelligence and the business/user communities. With respect to information-security standards and guidelines, there has been continuing concern with the lack of openness and accountability in policies formulated and implemented under executive order, rather than through the legislative process. It would be difficult to formulate a scenario in which increasing the defense/intelligence community's authority government-wide would result in more openness or assuage public concerns. (In the 1980s, concerns over NSDD-145's placement of governmental authority for unclassified information security within the defense/intelligence community led to enactment of the Computer Security Act of 1987.)

Oversight of the implementation of the Computer Security Act is also important to cryptography policy considerations. The cryptography-related FIPS still influence the overall market and the development of recent FIPS (e.g., the DSS and EES) demonstrates a mismatch between the intent of the act and its implementation by NIST and NSA (see pp. 160-183 of the 1994 OTA report). The attributes of these standards do not meet most users' needs, and their deployment would benefit from congressional oversight, both in the strategic context of a policy review and as tactical response to the Clinton Administration's escrowed-encryption initiative (see pp. 16-20 of the OTA report).

If the Computer Security Act is revisited, Congress might wish to redirect NIST's activities away from "picking technologies" for standards (i.e., away from developing product-oriented FIPS like the EES) and toward providing federal agencies with guidance on:

- the availability of suitable commercial technologies,
- interoperability and application portability, and
- how to make best use of existing hardware and software technology investments.

Also, targeting NIST's information-security activities toward support of OMB's proposed guidance (with its focus on end users and individual workstations) might enable NIST to be more effective despite scarce resources.