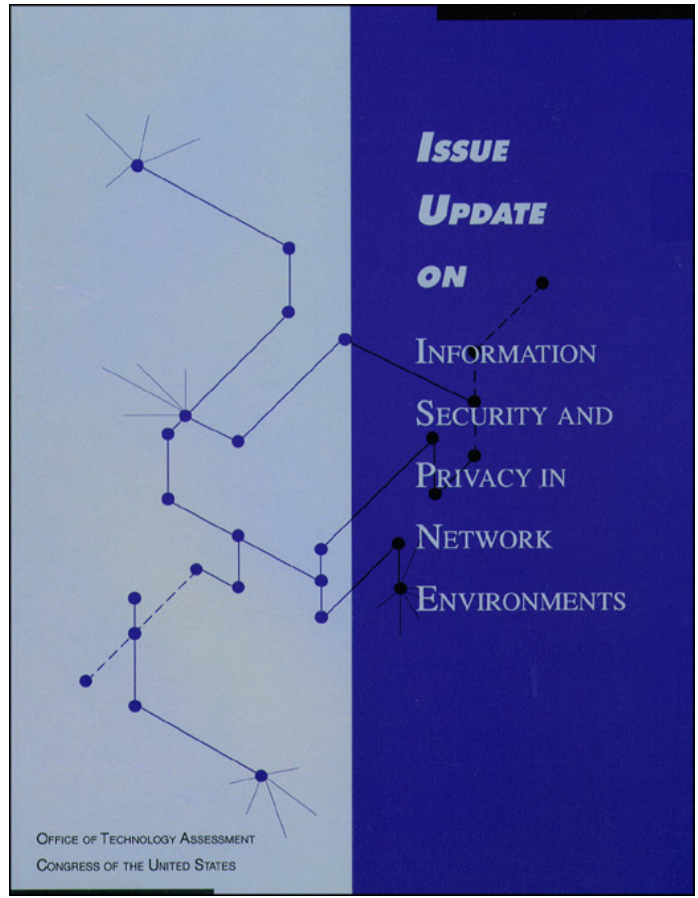
Issue Update on Information Security and Privacy in Network Environments

September 1995

OTA-BP-ITC-147

GPO stock #052-003-01416-5



Recommended Citation: U.S. Congress, Office of Technology Assessment, *Issue Update on Information Security and Privacy in Network Environments*, OTA-BP-ITC-147 (Washington, DC: U.S. Government Printing Office, June 1995).

Foreword

This background paper was prepared as part of the Office of Technology Assessment's follow-on assistance to the Senate Committee on Governmental Affairs, subsequent to release of the September 1994 OTA report *Information Security and Privacy in Network Environments.* The Committee requested additional informational and analytical assistance from OTA in order to prepare for hearings and legislation in the 104th Congress.

This background paper updates and develops some key issues that OTA had identified in its earlier report, in light of recent developments in the private sector and in government. During the course of this work, OTA found that the need for timely attention to the security of unclassified information has intensified in the months since the 1994 report was issued.

OTA appreciates the participation of many individuals without whose help this background paper would not have been possible. OTA received valuable assistance from workshop participants and many other reviewers and contributors from government, academia, and industry. The background paper itself, however, is the sole responsibility of OTA.



ROGER C. HERDMAN
Director

Workshop Participants, Reviewers, and Contributors

WORKSHOP PARTICIPANTS

James M. Anderson
LEXIS-NEXIS

Michael Baum
Independent Monitoring

Genevieve M. Burns
Monsanto Company

Robert H. Courtney, Jr.
RCI Inc.

L. Dain Gary
Computer Emergency Response Team

Bruce J. Heiman
Preston Gates Ellis & Rouvelas Meeds

Steven B. Lipner
Trusted Information Systems, Inc.

David P. Maher
AT&T Secure Communications Systems and Bell Laboratories

Fred Mailman
Hewlett Packard Company

Susan Nycum
Baker & McKenzie

David Alan Pensak
E.I. DuPont de Nemours, Inc.

Bill Poulos
Electronic Data Systems

Joel R. Reidenberg
Fordham University School of Law

Marc Rotenberg
EPIC

Corey D. Schou
Idaho State University

Frank W. Sudia
Bankers Trust Co.

Linda L. Vetter
Oracle Corp.

Bill Whitehurst
IBM Corp.

Dan Wilkenson
Computer Associates International, Inc.

Frederick Withington
GAO Advisory Council for Information Management and Technology

OTHER REVIEWERS AND CONTRIBUTORS

Maurice Cook
Bureau of Export Administration

Nanette DiTosto
Bankers Trust Co.

Dorothy Denning
Georgetown University

Bob Drake
National Security Agency

Lee Hollaar
University of Utah

Burt Kaliski
RSA Data Security, Inc.

F. Lynn McNulty
National Institute of Standards and Technology

Peter D. Saderholm
Security Policy Board Staff

Joseph Young
Bureau of Export Administration

Ed Roback
National Institute of Standards and Technology

Ed Springer
Office of Management and Budget

Note 1: OTA appreciates and is grateful for the valuable assistance and thoughtful critiques provided by the workshop participants and other reviewers and contributors. These individuals do not, however, necessarily approve, disapprove, or endorse this background paper. OTA assumes full responsibility for the background paper and the accuracy of its contents.

Note 2: Affiliations listed above were in effect at the time of the Workshop. Since that time, some have changed.

Project Staff

Peter D. Blair
Assistant Director, OTA
Industry, Commerce, and
International Security Division

Andrew W. Wyckoff
Program Director
Industry, Telecommunications,
and Commerce Program

ADMINISTRATIVE STAFF

Liz Emanuel
Office Administrator

Karry Fornshill
Secretary

Diane Jackson
Administrative Secretary

Karolyn St. Clair
PC Specialist

PRINCIPAL STAFF

JOAN D. WINSTON
Project Director

Miles Ewing
Contractor

PUBLISHING STAFF

Mary Lou Higgs
Manager

Denise Felix
Production Editor

Dorinda Edmondson
Typographer

Chris Onrubia
Senior Graphic Designer

Susan Hoffmeyer
Graphic Designer

Contents

1 Introduction and Summary 1

Introduction **2**
Information Security and Privacy in a Networked Society **4**
OTA Workshop Findings **14**
Issue Update **17**
Implications for Congressional Action **34**

2 Overview of the 1994 OTA Report on Information Security and Privacy 43

Information Security and Privacy in a Networked Society **43**
Review of the 1994 OTA Report **44**

3 Digest of OTA Workshop Discussion 65

Overview **65**
Information Security in the Private Sector **68**

4 Implications for Congressional Action 77

Update on Cryptography Initiatives **78**
Update on Business Perspectives **84**
Update on Privacy Legislation **88**
Update on Information-Security Policy Initiatives and Legislation **89**
Implications for Congressional Action **97**

APPENDICES

A Congressional Letter of Request 103

B Federal Information Security and the Computer Security Act 105

C U.S. Export Controls on Cryptography 116

D Summary of Issues and Options from the 1994 OTA Report 122

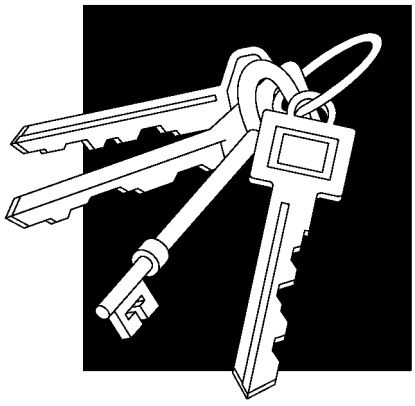
Index 133



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.

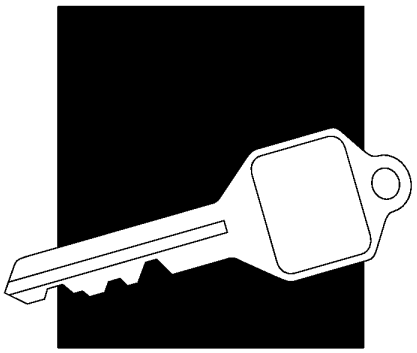
Also, targeting NIST's information-security activities toward support of OMB's proposed guidance (with its focus on end users and individual workstations) might enable NIST to be more effective despite scarce resources.

Overview of the 1994 OTA Report on Information Security and Privacy

2

This chapter highlights the importance of information security and privacy issues, explains why cryptography policies are so important, and reviews policy findings and options from the September 1994 OTA report *Information Security and Privacy in Network Environments*. Chapter 3 reviews the December 1994 OTA workshop and identifies key points that emerged from the workshop discussion, particularly export controls and the international business environment, federal cryptography policy, and information-security "best practices." Chapter 4 presents implications for congressional action, in light of recent and ongoing events.

This background paper is a companion and supplement to the September 1994 OTA report and is intended to be used in conjunction with that report. For the reader's convenience, however, pertinent technical and institutional background material, drawn from the September 1994 report and updated where appropriate, is included 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").



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. Government connectivity is also growing rapidly in scope and importance. Within the feder-

al government, effective use of information technologies and networks is central to government restructuring and reform.[1]

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.[2] 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.[3] 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.[4]

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.[5] 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.

REVIEW OF THE 1994 OTA REPORT

In September 1994, the Office of Technology Assessment released the report *Information Security*

---

[1] 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). See also Elena Varon, "Senate Panel Takes up IT Management Issues," *Federal Computer Week*, Feb. 6, 1995, p. 6; and 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 presented before the Committee on Governmental Affairs, U.S. Senate, Feb. 2, 1995.

[2] For example, measures to streamline operations via information technology require careful attention both to technical safeguards and to related institutional measures, such as employee training and awareness. Similarly, computer networks allow more interactivity, but the resulting transactional data may require additional safeguards to protect personal privacy.

[3] See Michael Neubarth et al., "Internet Security (Special Section)," *Internet World*, February 1995, pp. 31-72. See also Russell Mitchell, "The Key to Safe Business on the Net," and Amy Cortese et al., "Warding Off the Cyberspace Invaders," *Business Week*, Mar. 13, 1995, pp. 86, 92-93.

[4] 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 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), pp. 3-5, 25-32. Available from OTA Online via anonymous file transfer protocol (ftp://otabbs.ota.gov/pub/information.security/) or World Wide Web (http://www.ota.gov).

[5] 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.

and Privacy in Network Environments.[6] The report was prepared in response to a request by the Senate Committee on Governmental Affairs and the House Subcommittee on Telecommunications and Finance that OTA study the changing needs for protecting unclassified information and for protecting the privacy of individuals.[7] The request for the study was motivated by the rapid increase in connectivity within and outside government and the growth in federal support for large-scale networks. The report focused on safeguarding *information* in networks, not on the security or survivability of the networks themselves, nor on the reliability of network services to ensure information access.

The report identified policy issues and options 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. The 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 outline of policy issues and options in the last section of this chapter and the expanded discussion in appendix D).

Importance of Cryptography

Cryptography (see box 2-1) and related federal policies (e.g., regarding export controls and standards development) were a major focus of the report.[8] That focus was due in part from the widespread attention being given the so-called Clipper chip and the Clinton Administration's *escrowed-encryption* initiative. Escrowed encryption, or *key-escrow encryption,* refers to a cryptosystem in which the functional equivalent of a "spare key" must be deposited with a third party, in order to ensure easy access to decryption keys pursuant to lawful electronic surveillance. The Clinton Administration's escrowed-encryption initiative, first announced in 1993, required the "spare keys" to be held within the executive branch. The Escrowed Encryption Standard (EES), promulgated as a federal information processing standard (FIPS) in 1994, is approved for use in encrypting unclassified voice, fax, or data communicated in a telephone system.[9]

However, a focus on cryptography was inevitable, because in its modern setting, cryptography has become a fundamental technology with broad applications. Modern, computer-based cryptography and cryptanalysis began in the World War II era.[10] 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.[11]

Now, however, cryptography is a technology whose time has come—in the marketplace and in society. Cryptography is not arcane anymore. Despite two decades of growth in nongovernmental research and development, in the United States,

---

[6] Ibid.

[7] Ibid., pp. 5-6 and appendix A (congressional letters of request).

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

[9] 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.

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

[11] Although there has always been some level of nongovernmental cryptography research in the United States, from the end of WWII through the mid-1970s the federal government was almost the sole U.S. source of technology and know-how for modern cryptographic safeguards. The government's former near-monopoly in development and use of cryptography has been eroding, however.

BOX 2-1: Cryptograph

During the long history of paper-based "information systems" for commerce and communication, a number of safeguards were developed to ensure the confidentiality, integrity, and authenticity of documents and messages. These traditional safeguards included secret codebooks and passwords, physical "seals" to authenticate signatures, and auditable bookkeeping procedures. Mathematical analogues of these safeguards are implemented in the electronic environment. The most powerful of these are based on cryptography.

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

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

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

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

the federal government still does have 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) transforms a message or data files (called "plaintext") into a form (called "ciphertext") that is unintelligible without special knowledge of some secret information (called the "decryption key"). Figures 2-1 and 2-2 illustrate two common forms of encryption: 1) secret-key, or symmetric, encryption and 2) 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. In some cases (e.g., for archival records), when files or databases are encrypted, the keys have to remain cataloged and stored for very long periods of time.

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

BOX 2-1 (cont'd.): Cryptography

and decryption keys are different and one of them can be made public. With the advent of "public-key" techniques, cryptography also came into use for *digital signatures* that are of widespread interest as a means for electronically authenticating and signing commercial transactions like purchase orders, tax returns, and funds transfers, as well as ensuring that unauthorized changes or errors are detected.

Cryptanalysis is the study and development of various "codebreaking" methods to deduce the contents of the original plaintext message. The strength of an encryption algorithm is a function of the number of steps, storage, and time required to break the cipher and read any encrypted message, without prior knowledge of the key. Mathematical advances, advances in cryptanalysts, and advances in computing, all can reduce the security afforded by a cryptosystem that was previously considered "unbreakable" in practice.

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

Key *management* is fundamental and crucial to the security afforded by any cryptography-based safeguard. Key management includes generation of the encryption key or keys, as well as their storage, distribution, cataloging, and eventual destruction. If secret keys are not closely held, the result is the same as if a physical key is left "lying around" to be stolen or duplicated without the owner's knowledge. Similarly, poorly chosen keys may offer no more security than a lock that can be opened with a hairpin. Changing keys frequently can limit the amount of information or the number of transactions compromised due to unauthorized access to a given key. Thus, a well-thought-out and secure key-management infrastructure is necessary for effective use of encryption-based safeguards in network environments. Such a support infrastructure might include means for issuing keys and/or means for registering users' public keys and linking owner-registration certificates to keys so that the authenticity of digital signatures can be verified. This might be done by a *certificate authority* as part of a *public-key infrastructure.*

SOURCE: Office of Technology Assessment, 1995; drawing from OTA, *Information Security and Privacy in Network Environments* (OTA-TCT-606, September 1994), pp. 112-113 and sources cited therein.

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) 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).[12] These functions are critical for electronic commerce. Cryptographic techniques like digital signatures can also be used to help manage copyrighted material in electronic form. 13

[12]OTA, op. cit., footnote 4, pp. 69-77. See also Lisa Morgan, "Cashing In: The Rush Is on To Make Net Commerce Happen," *Internet World,* February 1995, pp. 48-51; and Richard W. Wiggirts, "Business Browser: A Tool To Make Web Commerce Secure," *Internet World,* February 1995, pp. 52-55.

[13] 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.

BOX 2-2: Encryption, Authentication, and Digital Signatures

Different cryptographic methods are used to authenticate users, protect confidentiality, and assure integrity of messages and files. Most systems use a combination of techniques to fulfill these functions.

Encryption

Cryptographic algorithms are either *symmetric* or *asymmetric,* depending on whether or not the same cryptographic key is used for encryption and decryption. The key is a sequence of symbols that determines the transformation from unencrypted *plaintext* to encrypted *ciphertext,* and vice versa.

"Symmetric" cryptosystems---also called secret-key or single-key systems—use the same key to encrypt and decrypt messages. Both the sending and receiving parties must know the secret key that they will use to communicate (see figure 2-1 in the main text). Secret-key algorithms can encrypt and decrypt relatively quickly, but systems that use only secret keys can be difficult to manage because they require a courier, registered mail, or other secure means for distributing keys. The federal Data Encryption Standard (DES) and the new Escrowed Encryption Standard (EES) each use a different secret-key algorithm.

"Asymmetric" cryptosystems---also called public-key systems—use one key to encrypt and a different, but mathematically related, public key to decrypt messages (see figure 2-2). For example, if an associate sends Carol a message encrypted with Carol's public key, in principle only Carol can decrypt it, because she is the only one with the correct private key This provides confidentiality and can be used to distribute secret keys, which can then be used to encrypt messages using a faster, symmetric cryptosystem (see figure 2-3).

The security of public-key systems rests on the authenticity of the public key (that it is a valid key for the stated individual or organization, not "recalled" by the owner or presented by an impostor) and the secrecy of the private key, much as the security of symmetric ciphers rests on the secrecy of the single key. Although the public key can be freely distributed, or posted in the equivalent of a telephone directory, its authenticity must be assured (e.g., by a certificate authority as part of a public-key infrastructure).

Commonly used public-key systems encrypt relatively slowly, but are useful for digital signatures and for exchanging the session keys that are used for encryption with a faster, symmetric cryptosystem. The Rivest-Shamir-Adleman (RSA) algorithm is a well-known, commercial public-key algorithm.

Authentication

The oldest and simplest forms of message authentication use "secret" authentication parameters known only to the sender and intended recipient to generate "message authentication codes. " So long as the secret authentication parameter is kept secret from all other parties, these techniques protect the sender and the receiver from alteration or forgery of a message by all such third parties. Because the same secret information is used by the sender to generate the message authentication code and by the receiver to validate it, these techniques cannot settle "disputes" between the sender and receiver as to what message, if any, was sent. For example, message authentication codes could not settle a dispute between a stockbroker and client in which the broker claims the client issued an order to purchase stock and the client claims he never did so.

For authentication, if a hypothetical user (Carol) uses her private key to sign messages, her associates can verify her signature using her public key. This method authenticates the sender, and can be used with hashing functions (see below) for a *digital signature* that can also check the integrity of the message.

Digital Signatures

Digital signatures provide a higher degree of authentication by allowing resolution of disputes. Although it is possible to generate digital signatures from a symmetric cipher like the DES, most interest centers on signature systems based on public-key cryptosystems.

BOX 2-2 (cont'd.): Encryption, Authentication, and Digital Signatures

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

In practice, digital signatures sign shorter "message digests" rather than the whole messages. In most public-key signature techniques, a one-way hash function is used to produce a condensed version of the message, which is then "signed. " For example, Carol processes her message with a '(hashing algorithm" that produces a shorter *message* digest—the equivalent of a very long checksum. Because the hashing method is a "one-way" function, the message digest cannot be reversed to obtain the message. Bob also processes the received text with the hashing algorithm and compares the resulting message digest with the one Carol signed and sent along with the message. If the message was altered in any way during transit, the digests will be different, revealing the alteration (see figure 2-4).

Signature Alternatives

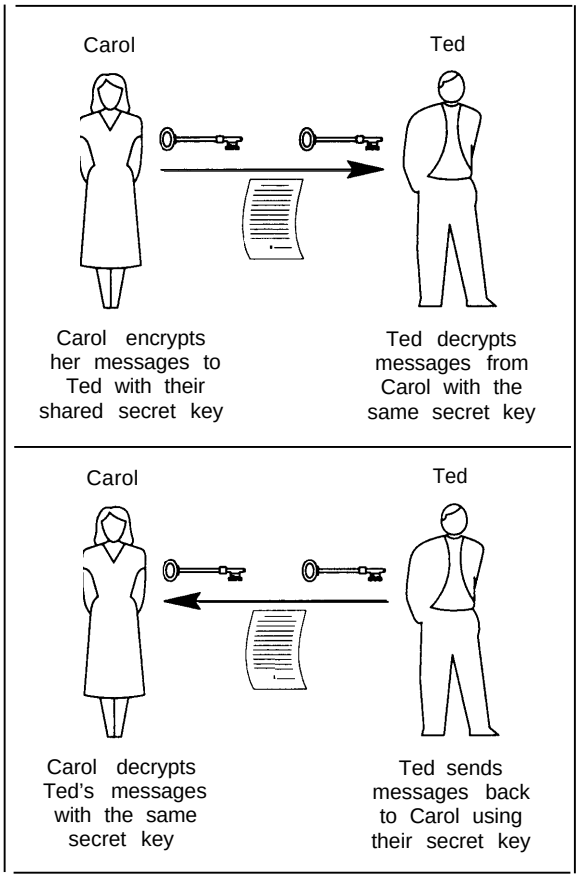
With the commercial RSA system, the signature is created by encrypting the message digest, using the sender's private key. Because in the RSA system each key is the inverse of the other, the recipient can use the sender's public key to decrypt the signature, thereby recovering the original message digest.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

The federal Digital Signature Standard (DSS) defines a somewhat different kind of public-key cryptographic standard for generating and verifying digital signatures. The DSS is to be used in conjunction with a federal hashing standard that is used to create a message digest, as described above. The message digest is then used, in conjunction with the sender's private key and the algorithm specified in the DSS, to produce a message-specific signature. Verifying the DSS signature involves a mathematical operation on the signature and message digest, using the sender's public key and the hash standard.

The DSS differs from the RSA digital signature method in that the DSS signature operation is not reversible, and hence can only be used for generating digital signatures. DSS signature verification is different than decryption. In contrast, the RSA system can encrypt, as well as do signatures. Therefore, the RSA system can also be used to securely exchange cryptographic keys that are to be used for confidentiality (e.g., "secret" keys for use with a symmetric encryption algorithm like the DES). This lack of encryption capability for secure key exchange was one reason why the government selected the DSS technique for the standard.

SOURCE: Office of Technology Assessment, 1995; drawing from OTA, *Information Security and Privacy in* Network Environments (OTA-TCT-606, September 1994), pp. 39 and 124-125 and sources cited therein See also U.S. Department of Commerce, National Institute of Standards and Technology, "Data Encryption Standard (DES), " FIPS Publication 46-2, Dec 30, 1993; "Digital Signature Standard (DSS)," FIPS Publication 186, May 19, 1994; and "Escrowed Encryption Standard (EES), " FIPS Publication 185, February 1994.

FIGURE 2-1: Secret-Key (Symmetric) Encryption



NOTE: Security depends on the secrecy of the shared key.

SOURCE: Office of Technology Assessment, 1994.

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. Absent government regulations, markets for cryptography would also be international. However, export controls create "domestic" and "export" markets for strong encryption products (see section on export controls below and also appendix C.[14] 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.[15]

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 five 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.

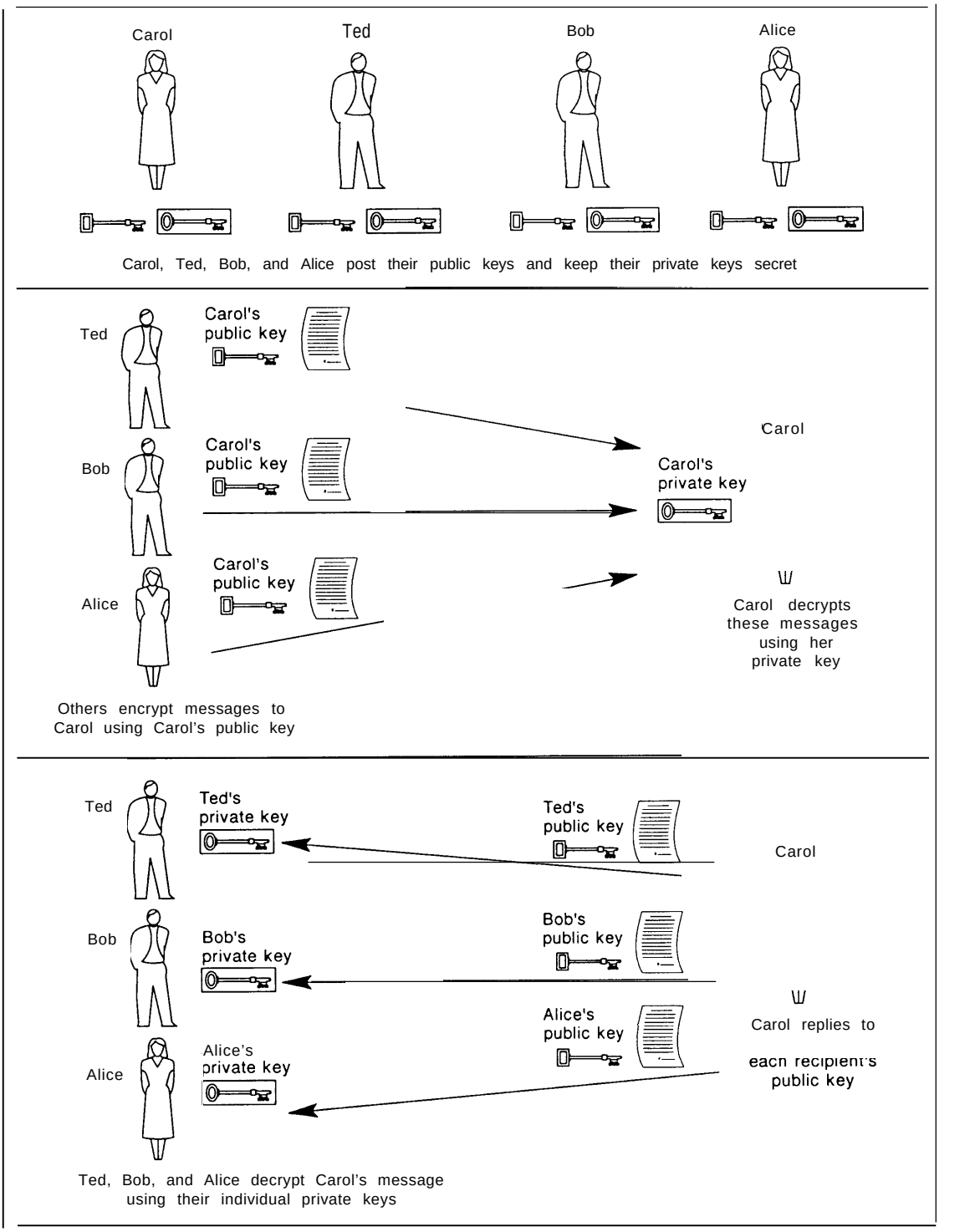
Previously, control of the availability and use of cryptography was presented as a national security issue focused outward, with the intention of maintaining a U.S. technological lead over other countries and preventing encryption devices from

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

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

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

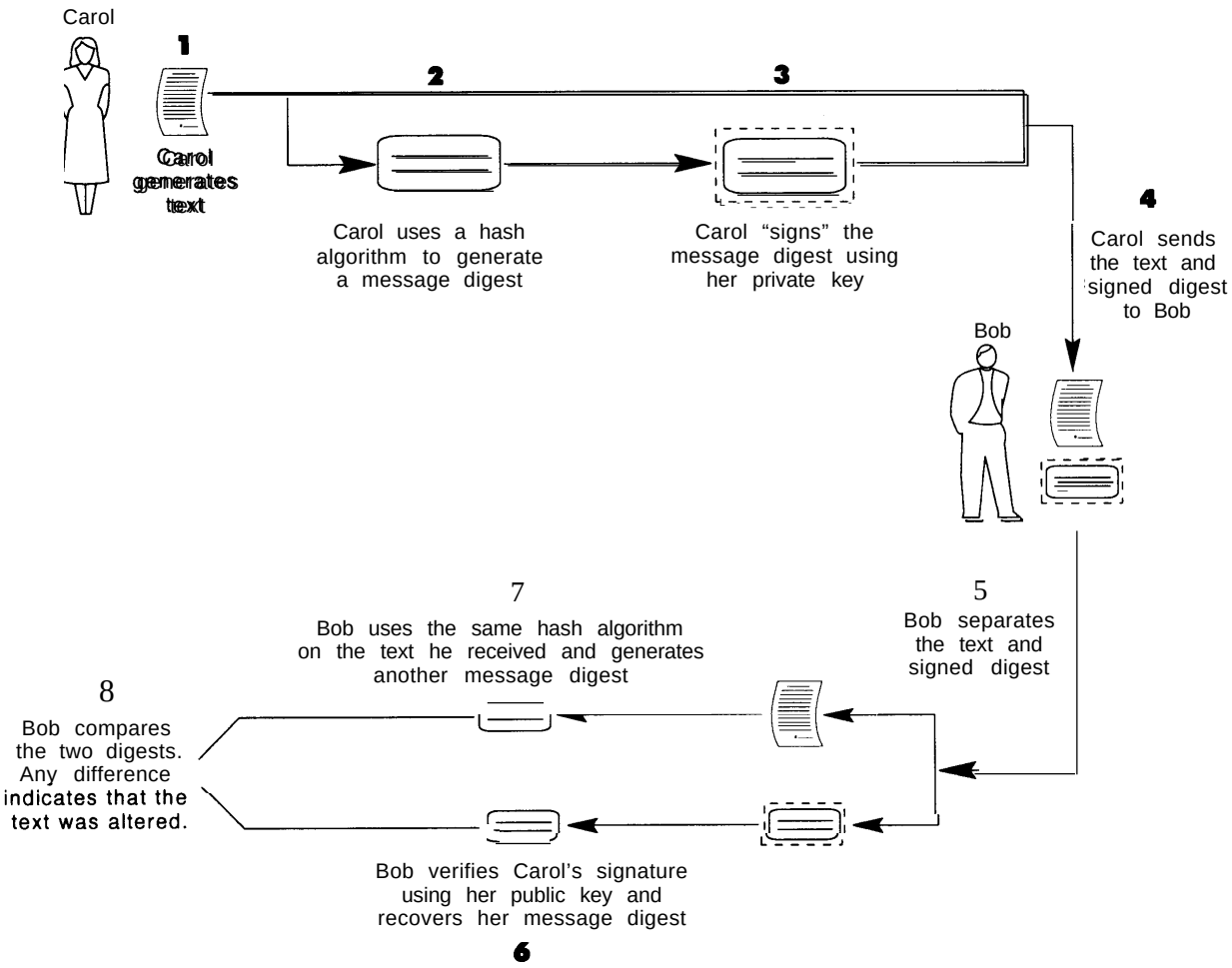
FIGURE 2-2: Public-Key (Asymmetric) Encryption



NOTE: Security depends on the secrecy of the private keys and the authenticity of the public keys.

SOURCE: Office of Technology Assessment, 1994

FIGURE 2-3: Example of a Hashing and Digital Signature Scheme



NOTE: Different methods for generating and verifying signatures (as in the federal Digital Signature Standard) are possible. Measures to protect the signature and text may also be used.

SOURCE: Office of Technology Assessment, 1994

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. 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. There is also growing recognition of potentials for misuse, such as by disgruntled employees as a means to sabotage an employer's databases. 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-es-

crow encryption, that are intended to preserve U.S. law enforcement and signals-intelligence capabilities (see box 2-3).

Standards-development and export-control issues underlie a long history of concern over leadership and responsibility (i.e., *"who should be in charge?"* and *"who is in charge?"*) for the security of unclassified information government-wide.[17] Most recently, these concerns have been revitalized by proposals (presented by the Clinton Administration's Security Policy Board staff) to centralize information-security authorities government-wide under joint control of the Office of Management and Budget (OMB) and Department of Defense (DOD) (see discussion in chapter 4).[18]

Other manifestations of these concerns can be found in the history of the Computer Security Act of 1987 (Public Law 100-235—see the next section 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[19] and Digital Signature Standard (DSS)[20] 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).

The Escrowed Encryption Standard has been promulgated by the Clinton Administration as a voluntary federal encryption standard (i.e., a voluntary, rather than mandatory, FIPS). The EES announcement noted that the standard does not mandate the use of escrowed-encryption devices by government agencies or the private sector; 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).[21]

The EES is intended for use in encrypting unclassified voice, facsimile, and computer information communicated over a telephone system. The encryption algorithm (called Skipjack) specified in the EES can also be implemented for data communications in computer networks. At this writing, there is no FIPS specifying use of Skipjack as a standard algorithm for data communications or file encryption.

However, DOD is using Skipjack for encryption in computer networks (e.g., in the "FORTEZZA" PCMCIA card). As of April 1995, according to the National Security Agency (NSA), approximately 3,000 FORTEZZA cards have been produced and another 33,000 are on contract; some 100 to 200 are being tested and used in applications development by various DOD organizations, mostly in support of the Defense Message System.[22] According to the NSA, plans call for

---

[17] Ibid., pp. 8-20 and chapter 4.

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

[19] See box 2-3 and OTA, op. cit., footnote 4, ch. 4.

[20] See box 2-2 and OTA, ibid., appendix C.

[21] 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.

[22] Bob Drake, Legislative Affairs Office, NSA, personal communication, Apr. 7, 1995.

BOX 2-3: The Escrowed Encryption Standard

The federal Escrowed Encryption Standard (EES) was approved by the Commerce Department as a federal information processing standard (FIPS) in February 1994.[1] According to the standard (described in FIPS PUB 185), the EES is intended for voluntary use by all federal departments and agencies and their contractors to protect unclassified information. Implementations of the EES are subject to State Department export controls. In 1994, however, the Clinton Administration indicated that encryption products based on the EES would be exportable to most end users and that EES products will qualify for special licensing arrangements.[2]

The National Security Council, Justice Department, Commerce Department, and other federal agencies were involved in the decision to propose the EES, according to a White House press release and information packet dated April 16, 1993, the day the EES initiative was announced. The EES algorithm is said to be stronger than the Data Encryption Standard (DES) algorithm, but able to meet the legitimate needs of law enforcement agencies to protect against terrorists, drug dealers, and organized crime.[3]

EES Functions

The EES is intended to encrypt voice, fax, and computer data communicated in a telephone system. It may, on a voluntary basis, be used to replace DES encryption devices now in use by federal agencies and contractors. Other use by the private sector is voluntary. The EES specifies a symmetric encryption algorithm, called "Skip jack." The Skipjack algorithm is a classified algorithm, developed by the National Security Agency (NSA) in the 1980s.[4] An early implementation was called Clipper, hence the colloquial use of Clipper or Clipper Chip to describe the EES technology.[5]

The EES also specifies a method to create a Law Enforcement Access Field (LEAF), in order to provide for easy decryption when the equivalent of a wiretap has been authorized.[6] The Skipjack algorithm and LEAF creation method are implemented only in electronic devices (i.e., very-large-scale integration chips). The chips are "highly resistant" to reverse engineering and will be embedded in tamper-resistant cryptographic modules that approved manufacturers can incorporate in telecommunications or computer equipment. The chips are manufactured by VLSI Logic and are programmed with the algorithms and keys by Mykotronx. The programming is done under the supervision of the two "escrow agents" (see below).

---

[1] See Federal Register, vol. 59, Feb. 9, 1994, pp. 5997-6005.

[2] Martha Harris, Deputy Assistant Secretary of State for Political-Milltary Affairs, "Statement on Encryption-Export Control Reform, " Feb. 4, 1994 *[OTA note The anticipated reforms had not all materialized as of this writing.]*

[3] Because the EES algorithm IS classified, the overall strength of the EES cannot be examined except under security clearance (see below). Thus, unclassified, public analyses of its strengths and weaknesses are not possible. The only public statements made by the Clinton Administration concerning the strength of the EES relative to the DES refer to the secret-key size: 80 bits for the EES versus 56 bits for the DES

[4] The NSA specifications for Skipjack and the LEAF creation method are classified at the Secret level. (OTA project staff did not access these, or any other classified information.)

[5] The Clipper Chip implementation of Skipjack is for use in secure telephone communications. An enhanced escrowed-encryption chip with additional functions, called Capstone, is used in data communications. Capstone is in the FORTEZZA PCMCIA card being used in the Defense Message System

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

BOX 2-3 (cont'd.): The Escrowed Encryption Standard

After electronic surveillance has been authorized, the EES facilitates law enforcement access to encrypted communications. This is accomplished through what is called a "key escrowing" scheme. Each EES chip has a chip-specific key that is split into two parts after being programmed into the chips. These parts can be recombined to gain access to encrypted communications. One part is held by each of two designated government keyholders, or "escrow agents." Attorney General Reno designated the National Institute of Standards and Technology (NIST) and the Treasury Department's Automated Systems Division as the original escrow agents. The only public estimate (by NIST, in early 1994) of the costs of establishing the escrow system was about $14 million, with estimated annual operating costs of$16 million.

When surveillance has been authorized and the intercepted communications are found to be encrypted using the EES, law enforcement agencies can obtain the two parts of the escrowed key from the escrow agents. These parts can then be used to obtain the individual keys used to encrypt (and, thus, to decrypt) the telecommunications sessions of interest.[7] The LEAF is transmitted along with the encrypted message; it contains a device identifier that indicates which escrowed keys are needed.

EES History

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

During the review period, the Skipjack algorithm was evaluated by outside experts, pursuant to President Clinton's direction that "respected experts from outside the government will be offered access to the confidential details of the algorithm to assess its capabilities and publicly report their findings. " Five reviewers accepted NIST's invitation to participate in a classified review of Skipjack and publicly report their findings: Ernest Brickell (Sandia National Laboratories), Dorothy Denning (Georgetown University), Stephen Kent (Bolt Beranek and Newman, Inc.), David Maher (AT&T), and Walter Tuchman (Amperif Corp.). Their interim report on the algorithm itself found that: 1) there is no significant risk that Skipjack will be broken by exhaustive search in the next 30 to 40 years; 2) there is no significant risk that Skipjack can be broken through a shortcut method of attack; and 3) while the internal structure of Skipjack must be classified in order to protect law enforcement and national security objectives, the strength of Skipjack against a cryptanalytic attack does not depend on the secrecy of the algorithm.[9]

---

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

[8] *Federal Register* (Feb. 9, 1994), op. cit. footnote 1, pp. 5998-6002.

[9] E. Brickell (Sandia National Laboratories) et al., "SKIPJACK Review Interim Report-The SKIPJACK Algorithm, " July 28, 1993. See also "Fact Sheet—NIST Cryptography Activities," Feb. 4, 1994

(continued)

BOX 2-3 (cont'd.): The Escrowed Encryption Standard

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

In early 1995, an alternative, commercial key-escrow encryption system being developed by Trusted Information Systems, Inc. (TIS) was undergoing internal government review to determine whether such an approach could meet national security and law enforcement objectives. The TIS key-escrow system does software-based escrowing and encryption using the "triple-DES" version of the Data Encryption Standard.[13] The initial version of the system is designed for use in encrypting files or email, but the TIS approach could also be used for real-time telecommunications.

In January 1995, AT&T Corp. and VLSI Technology, Inc., announced plans to develop chips implementing the RSA algorithm and "triple DES" for encryption. The chips would be used in a personal computers, digital telephones, and video decoder boxes.[14]

[10] Ibid., and *Federal Register (* Feb. 9, 1994), OP. Cit., footnote 1.

[11] Ibid.

[12] White House press release and enclosures, Feb. 4, 1994, "Working Group on Encryption and Telecommunications. "

[13] Stephen T. Walker et al., "Commercial Key Escrow: Something for Everyone Now and For the Future, " TIS Report No. 541, Trusted Information Systems, Inc., Jan. 3, 1995.

[14] Jared Sandberg and Don Clark, "AT&T, VLSI Technology To Develop Microchips That Offer Data Security, *The Wall Street Journal,* Jan. 31, 1995.

SOURCE: Off Ice of Technology Assessment, 1995; drawing from OTA, *Information Security And Privacy in Networked Environments* (OTA-TCT-606, September 1994), pp. 118-119 and sources cited therein and below.

eliciting and aggregating bulk orders for FORTEZZA in order to support the award of a large-scale production contract in the fall, ideally for 200,000 to 400,000 units in order to achieve the target unit price of $100.[23]

The algorithm specified in the EES has not been published. The secret encryption key length for Skipjack is 80 bits; a key-escrowing scheme is built into ensure "lawfully authorized" electronic surveillance.[24] The algorithm is classified and is intended to be implemented only in tamper-resistant, hardware modules.[25] This approach makes the confidentiality function of the Skipjack en-

[23] Ibid. According to the NSA, unit prices for FORTEZZA cards in small quantities are on the order of $150, of which about $98 is for the Capstone chip. The Capstone chip implements the Skipjack algorithm, plus key-exchange and digital-signature (DSS) functions.

[24] *Federal Register,* ibid., p. 6003.

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

cryption 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 federal Data Encryption Standard was first approved in 1976 and was most recently reaffirmed in 1993. The DES specifies an algorithm that can be used to protect unclassified information, as needed, while it is being communicated or stored.[26] The DES algorithm has been made public (i.e., it has been published). When the DES is used, users can generate their own encryption keys; the secret encryption key for DES is 56 bits long. The DES does not require the keys to be "escrowed" or deposited with any third party.

The 1993 reaffirmation of the DES—now in software, as well as hardware and firmware implementations—may be the last time it is reaffirmed as a federal standard. FIPS Publication 46-2 ("Data Encryption Standard") noted that the algorithm will be reviewed within five years to assess its adequacy against potential new threats, including advances in computing and cryptanalysis:

> At its next review (1998) [the DES algorithm] will be over twenty years old. NIST [National Institute of Standards and Technology] will consider alternatives which offer a higher level of security. One of these alternatives may be proposed as a replacement standard at the 1998 review.[27]

Given that the Skipjack algorithm was selected as a standard (the EES) 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*. In "triple DES," the 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 112-bit DES key. Therefore, nongovernmental experts consider that triple DES "appears inviolate against all adversaries for the foreseeable future."[28] There is, however, no FIPS for triple-encryption DES.

Unlike the EES algorithm, the algorithm in the federal Digital Signature Standard has been published.[29] 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.[30] 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.[31] At present, there is no FIPS for key exchange.

While other means of exchanging electronic keys are possible,[32] none is so mature as public-

---

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

[27] Ibid., p. 6.

[28] Martin Hellman, Professor of Electrical Engineering, Stanford University, personal communication, May 24, 1994; also see box 4-3 of the 1994 report.

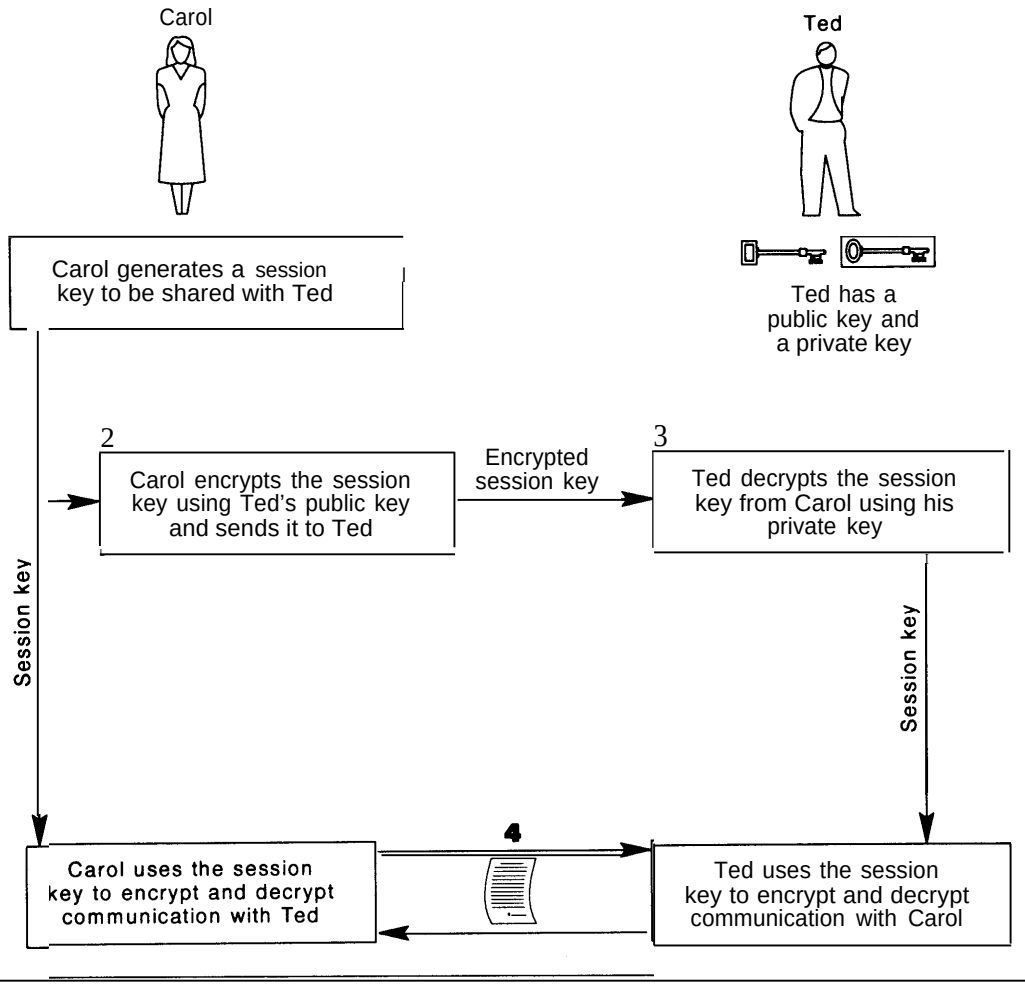
[29] See appendix C of OTA, op. cit., footnote 4, for a history of the DSS.

[30] According to F. Lynn McNulty, NIST Associate Director for Computer Security, the rationale for adopting the technique used in the 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.)

[31] 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.

[32] 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.

FIGURE 2-4: Secret-Key Distribution Using Public-Key Cryptography



NOTE: Security depends on the secrecy of the session key and private keys, as well as the authenticity of the public keys.

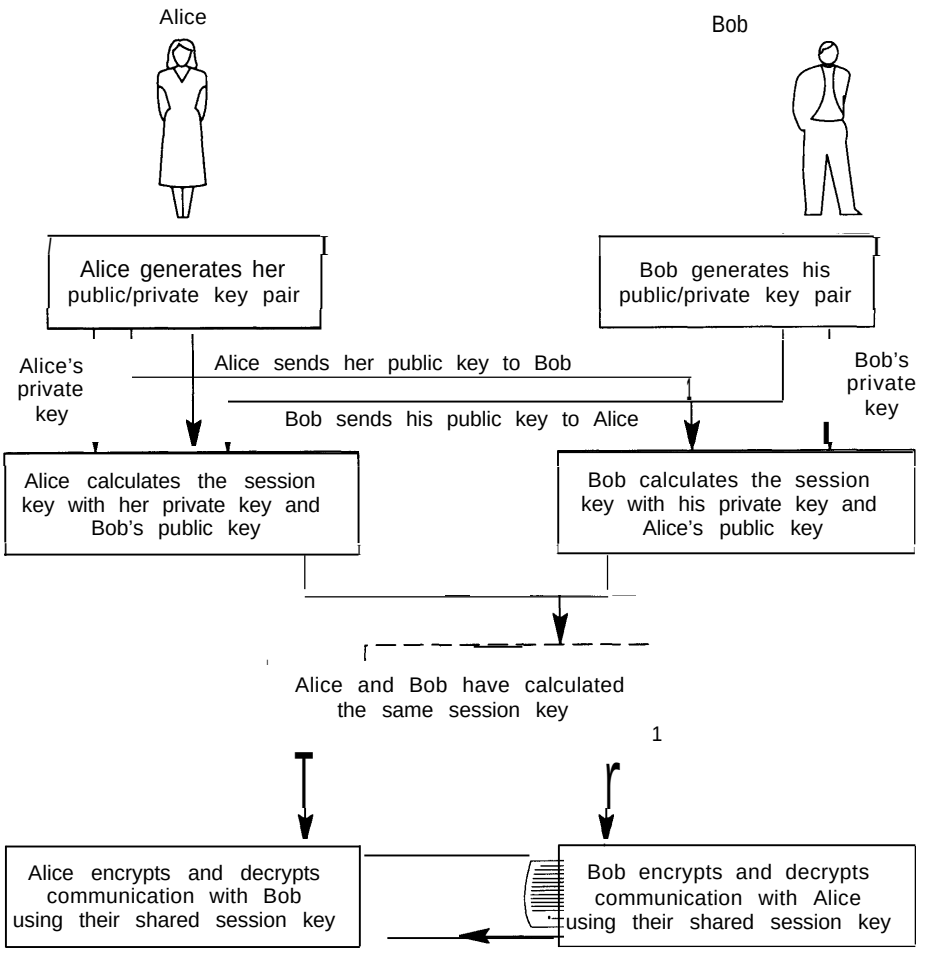
SOURCE: Office of Technology Assessment, 1994.

key technology. In contrast to the technique chosen for the DSS, the technique used in the most widely used commercial digital signature system (based on the Rivest-Shamir-Adleman, or RSA, 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 (see figure 2-4). Another public-key technique, called the Diffie-Hellman method, can also be used to generate encryption keys (see figure 2-5), but does not encrypt.[33]

The 1994 OTA report concluded that both the EES and the DSS are federal standards that are part of a long-term control strategy intended to re-

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

FIGURE 2-5: Diffie-Hellman Key Exchange



NOTE: An authentication scheme for the public keys may also be used

SOURCE: Office of Technology Assessment, 1994.

tard the general availability of "unbreakable" or "hard to break" encryption within the United States, for reasons of national security and law enforcement.[34] OTA viewed the EES and DSS 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 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 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.

[34]See OTA, op.cit., footnote 4, ch. 4.

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 NIST and 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).[35]

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.

Specifically, the Computer Security Act assigned responsibility for developing government-wide, computer-system security standards (e.g., the FIPS) and guidelines and security-training programs to the National Bureau of Standards (NBS). NBS is now the National Institute of Standards and Technology, or NIST. 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.[36] NIST can draw on the technical expertise of the National Security Agency in carrying out its responsibilities, but the NSA's role according to Public Law 100-235 is an advisory, rather than leadership, one.

Section 21 of the Computer Security Act established a Computer System Security and Privacy Advisory Board. The board, appointed by the Secretary of Commerce, is charged with identifying emerging safeguard issues relative to computer systems security and privacy, advising the NBS (NIST) and Secretary of Commerce on security and privacy issues pertaining to federal computer systems, and reporting its findings to the Secretary of Commerce, the Director of OMB, the Director of NSA, and 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.

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. For example, the government made an early commitment to the Open Systems Interconnection (OSI) protocols for networking, but it is the ubiquitous Transmission Control Protocol/Internet

---

[35] Ibid., 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.

[36] Tha 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.

Protocol (TCP/IP) that has enjoyed wide use throughout the world in the Internet and other networks. However, the FIPS usually influence the technologies used by federal agencies and provide a basis for interoperability, thus creating a large and stable, "target market" for safeguard vendors. If the attributes of the standard technology are also applicable to the private sector and the standard has wide appeal, an even larger but still relatively stable market should result. The technological stability means that firms compete less in terms of the attributes of the fundamental technology and more in terms of cost, ease of use, and so forth. Therefore, firms need to invest less in research and development (especially risky for a complex technology like cryptography) and in convincing potential customers of product quality. 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 DES as a stable and certified technology—at a time when the commercial market for cryptography-based safeguards for unclassified information was emerging—stimulated supply and demand. Although the choice of the algorithm was originally controversial due to concerns over NSA's involvement, the DES gained wide acceptance and has been the basis for several industry standards, in large part because it was a published standard that could be freely evaluated and implemented. Although DES products are subject to U.S. export controls, DES technology is also widely available around the world and the algorithm has been adopted in several international standards. The process by which the DES was developed and evaluated also stimulated private sector interest in cryptographic research, ultimately increasing the variety of commercial safeguard technologies.

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 related technologies 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 its lack of appeal. But, if the EES and related technologies (e.g., for data communications) 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.[37]

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 (see appendix C).[38] The United States has two regulatory regimes for exports, depending on whether the item to be exported is military in nature, or is "dual-use," having both civilian and military uses. These regimes are ad-

[37] Ibid., pp. 128-132. A large, stable, lucrative federal market could divert vendors from producing alternative, riskier products; product availability could draw private sector customers.

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

ministered 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 "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.[39]

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.[40] 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.[41] 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.[42]

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 on the degree of success of these export controls[43] and the necessity for maintaining strict controls on strong encryption[44] in the face of for-

---

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

[40] To ease some of these burdens, the State Department announced new licensing procedures on Feb. 4, 1994. These changes were expected 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).

[41] 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.

[42] OTA, op. cit., footnote 4, pp. 154-160. Some other countries do have stringent export and/or import restrictions.

[43] For example, the Software Publishers Association (SPA) 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 4, pp. 156-160.

[44] 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 a public-key encryption program developed by Phil Zimmerman. Variants of the PGP software (some of which 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.)

eign supply and networks like the Internet that seamlessly cross national boundaries.

Appendix C 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.[45] The new rule implements one of the reforms applicable to encryption products that were announced on February 4, 1994 by the State Department (see footnote 47 below and also chapter 4 of the 1994 OTA report). It established a new licensing procedure to permit U.S. encryption manufacturers to make multiple shipments of some encryption items covered by Category XIII(b)(1) of the Munitions List (see appendix C) directly to end users in approved countries, without obtaining individual licenses.[46] Other announced reforms, still to be implemented, include special licensing procedures allowing export of key-escrow encryption products to "most end users."[47] The ability to export strong, key-escrow encryption products would presumably increase the appeal of escrowed-encryption products 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.[48]

At the end of the 103d Congress, the 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."[49]

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.[50] As part of the study, NSA is determining the foreign availability of en-

---

[45] 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.

[46] Category XIII(b)(1) covers "Information Security Systems and equipment, cryptographic devices, software and components specifically designed or modified therefore," in particular, "cryptographic and key-management systems and associated equipment, subcomponents, and software capable of maintaining information or information-system secrecy/confidentiality."

[47] 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 4, pp. 159-160.

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

[49] Vice President Al Gore, letter to Representative Maria Cantwell, July 20, 1994. See OTA, op. cit., footnote 4, pp. 11-13.

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

cryption products. The study is scheduled to be delivered to the National Security Council (NSC) by July 1, 1995. According to the Council, it is anticipated that there will be both classified and unclassified sections of the study; there may be some public release of the unclassified material.[51] In addition, an ongoing National Research Council 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.[52] At this 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 does 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 in chapter 4).

Overview of Issues and Options

As noted above, the 1994 OTA report *Information Security and Privacy in Network Environments* focuses on three sets of policy issues:

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.

Appendix E of this paper, based on chapter 1 of the 1994 report, reviews the set of policy options, about two dozen, developed by OTA. 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.

Two key questions underlying consideration of many of these options—in particular, those 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.

---

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

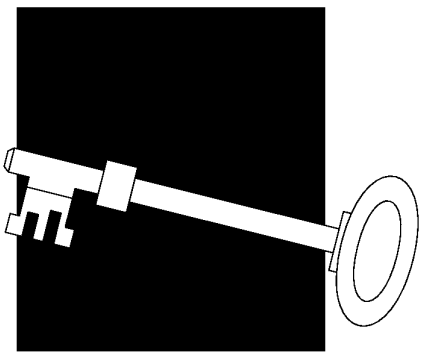
[52] For information about the NRC study, which was mandated by Public Law 103-160, contact Herb Lin, National Research Council, 2101 Constitution Avenue, N.W., Washington, DC, 20418 (crypto@nas.edu). See discussion in chapter 1 and 4 of OTA, op. cit., footnote 4.

Digest of OTA Workshop Discussion 3

At the request of the Senate Committee on Governmental Affairs, the Office of Technology Assessment (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 report *Information Security and Privacy in Network Environments*.[1] The purpose of the workshop was to hear the reactions from the business and network-user communities to the issues OTA had identified, as well as their priorities for any government actions. This chapter will review the workshop discussion and identify major themes that emerged, particularly 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.

OVERVIEW

Workshop participants came from the business, legal, university, and public-interest communities. Individuals' areas of experience and expertise included computer, telecommunication, and security technologies; information-security education and practice in the private and public sectors; management; and law. About half of the 20 participants had prior involvement with the 1994 OTA security and privacy report, as advisory panel members for the assessment, workshop participants, and/or reviewers.



[1] 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).

The workshop participants also served as external reviewers for this background paper. *The workshop participants do not, however, necessarily approve, disapprove, or endorse this background paper.* OTA assumes full responsibility for the background paper and the accuracy of its contents.

One workshop objective was to gauge participants' overall reactions to the 1994 OTA report on security and privacy. Another objective 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 below). However, the intent of the workshop was not to rehash the issues and controversies described in the report, but rather to build on the report and push beyond it. A goal for the workshop was for participants to identify—as specifically as possible—areas ripe for congressional action.

To spark their thinking and help focus the day's discussion, participants received a set of discussion topics and questions in advance (see box 3-1), along with a copy of the 1994 report. 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.

The spirited and lively workshop discussion identified linkages among a wide variety of the topics and questions posed by OTA. The range of discussion included cryptography policies (especially export controls on cryptography), information security in the private sector, privacy protections, safeguarding proprietary information and intellectual property, and business needs in the international marketplace.

OTA has identified some themes from the day's discussion that have particular significance, especially in the context of current developments, for congressional consideration of information-security issues and options identified in the 1994 OTA report. These themes, which are explored in chapter 4 of this background paper, 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 intense dissatisfaction on the part of the private sector with the lack of openness and progress in resolving cryptography-policy issues;
- the mismatch between the federal standards process for cryptography-related federal information processing standards (FIPS) and private sector needs for exportable, cost-effective safeguards;
- the mismatch between the intent of the Computer Security Act and its implementation;
- the distinction between security policies and guidelines for implementing these policies;
- the need for technological flexibility in implementing security policies; and
- 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 remainder of this chapter highlights major points and opinions expressed by the workshop participants, while attempting to convey a sense of the variety of positions propounded. It is important to note that this presentation is not intended to represent conclusions reached by the participants; moreover, the reader should not infer any general consensus, unless consensus is specifically noted.

Cryptography Policy and Export Controls

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.

BOX 3-1: Areas of Inquiry for Workshop

The marketplace for information safeguards (supply and demand)

- What factors and considerations affect the demand for and supply of safeguard tools?
- With respect to personal privacy, are database owners/custodians and information system administrators sufficiently willing and able to protect privacy?
- Is there a market failure that requires government intervention?

Information-security "best practice," training, and technology tools

- What is the state of "best practice" in information security (and implications for agencies and Office of Management and Budget guidance)?
- Security training and awareness.
- Technology tools for securing networks and data.

Impacts of federal policies on business and the public

- What is the likely impact of federal policies and initiatives on business? On agency operations and interactions with the private sector?
- Impact of cryptography policies on business.
- Electronic commerce and contracts.

What should Congress do-and when?

- Prioritization of problem areas or needs identified in discussion.
- Is there a possible problem of "having the tail wag the dog"?
- What are specific solutions for high-priority problems/needs?

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."

U.S. export policy restrictions on products implementing the Data Encryption Standard (DES) and/or the Rivest-Shamir-Adleman (RSA) algorithm are viewed by several participants as anticompetitive and likely to stall U.S. information technology, because they frustrate both the multinational companies' need to communicate securely worldwide and the U.S. vendors who furnish secure communication products. Multinationals are forced to go elsewhere and have suppliers build for them abroad, while U.S. vendors face an artificially limited market. (These products can then be used overseas and also be imported for use in the United States.)

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. They noted 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. Many participants also viewed export controls as the single biggest obstacle to establishing international standards for information safeguards; one noted the peculiarity of picking a national standard and then trying to restrict its use internationally.

Participants also 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.[2] 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.

Some participants also noted the importance of increased oversight of the Computer Security Act of 1987 (Public Law 100-235), as well as possible redirection of National Institute of Standards and Technology (NIST) activities (e.g., collecting information about what industry is doing, pointing out commonalities and how to interoperate, rather than picking out a "standard").

INFORMATION SECURITY IN THE PRIVATE SECTOR

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, was noted as very important by several participants. Sound security policies as a foundation for good practice were described as technology neutral, consistent across company cultures, minimalist, and as absolutes. Much was made of technology-neutral policies because properly applied, they do not prescribe implementations, are not easily obsoleted by changes in technology or business practices, and allow for local customization of implementations to meet operational requirements.

Information-Security Policies and "Best Practices"

There was general agreement that direct support by top management (e.g., the chief executive officer and board of directors of a corporation) and upper-management accountability are central to successful implementation of security policy. Many participants felt that tying responsibility for the success of security policies—and for the consequences of security incidents—to upper management is critical. Many considered it vital that the managers not be insulated from risk. According to one participant, it is important to educate managers on active risk acceptance; another suggested that their divisions could be held financially responsible for lost information.

In some of the companies represented, security policy has been refined to the point of "Thou shalt . . . not how thou shalt." Security managers are charged with developing something resembling the "Ten Commandments" of security. 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 aspects 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. 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

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

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 roadblocks frustrating more robust security for information and information systems. The primary roadblock 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.

Availability of Secure Products

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. As described above, 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. Many felt the market will develop security standards and secure systems if left to its own devices; others took issue with this position.

Some participants said there are problems in the marketplace. They asserted that many computer products are not designed with security in mind and cannot be made secure easily or cheaply. In particular, the UNIX operating system and the Internet architecture were cited as examples of products designed without "built-in" security. Some suggested that today's fierce price competition forces product vendors to disregard security features in favor of cost savings, leaving the purchaser to add security to the system retroactively, at a much higher cost.

The perceived propensity for security to be deferred in order to cut costs had one or two participants questioning the ability of the market to develop reasonably priced secure products for information systems and whether government action is needed to lead the market in the "right" direction—for example, through standards for federal procurements or regulations setting baseline product requirements. Though most participants seemed to agree that many products have been built without security features and that retrofitting a system with security is expensive and difficult, there was strong sentiment from industry representatives that the market should be left alone. Many participants described government interventions into the market, such as export controls and the Escrowed Encryption Standard (EES, or Clipper), as economically detrimental, and saw nothing to indicate that interventions would be more beneficial in the future.

Some pointed out a distinction between the ability of large businesses and small businesses to purchase products that incorporate security. Large businesses are able to demand more security features because of the size of their operations; while smaller companies must often individually purchase and configure a basic product, which may have been designed without security in mind.

Implicit in the discussion of the ability of the market to produce secure products is the extent of demand for them. Those arguing that market forces will develop secure systems stated, basically, that when buyers demand secure products, secure products will be available. Participants from vendor companies were especially adamant about the strength of the relationship between themselves and the industry users. (One example of user efforts to work with vendors to develop more security-oriented products is a group called Open User Recommended Solutions (OURS), which has recently developed a single sign-on product description.) Those who felt the market will not develop secure products in the near future feel that the demand for inexpensive products will con-

tinue to outweigh demand for security, and/or noted the demand-segmenting effects of export controls.

Some participants pointed out that the reason security concerns defer to price concerns is the inability to quantify the value of good security. Some noted this as a prevalent problem when attempting to convince upper management of the need for security. Lack of reported breaches, the inability to evaluate successful security, and the lack of a direct cost/benefit analysis all lead to an unclear assessment of need. This in turn reduces the demand, which drives the market to ignore security.

Training

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 system—for 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. Some companies develop elaborate video presentations to ensure that training is consistent throughout the various company cultures. Some participants felt that employees must be trained in technology; believing that, if users do not understand the technologies they have incorporated into their business, then they will be pressed to do what is necessary to implement security policies.

The necessity for impressing upon employees their role in information security is paramount. Because the average individual tends to not recognize the importance of training, it falls to management to demonstrate its value. To this end, several participants emphasized the importance of demonstrating the value of training to management. Many felt that much of the responsibility for getting management interested in training rested with the program manager. Like other elements of information security, financial departments have difficulty quantifying the value of training. Some point out that "an insurance" policy is a poor model, because there are no guarantees, nor are the risks easily quantifiable. Some suggested it will take a crisis to convince upper management of the need to effectively train employees and that anecdotal evidence is the best tool in the absence of hard definable numbers. This view was not universally accepted.

Common Themes

A common thread to the discussion of information-security practices is the necessity for a heightened awareness of security needs by upper management. Making management aware of the danger of and propensity for financial loss due to lax security is vital to security policy, product availability, and the training issue. Some participants felt that the inability to set up a cost justification formula for information security is a major impediment to convincing management of the need for it. In addition, the difficulty in evaluating the success of a security program limits a security officer in making a case to management.

A proposed solution to this problem is the establishment of an agreed-upon body of knowledge or "common checklist" for security officers to compare their company policies against. There is a large core of commonality in security awareness, training, and education. If made legally binding, or part of industry consensus as to what constitutes "prudent practice," such a checklist would also tie directly into the liability issues as well as a host of other problems facing companies. For example, when organizations outsource, contractual specifications are needed to ensure adequate security coverage. If there were a well-known and accepted "common checklist" for security, then it would be easier to develop contractual specifica-

tions without revealing too much of your operations or levels of security to the contractor.

Domestic and International Privacy Issues

Consumers are increasingly concerned with control of personal and transactional data and are seeking some protection from potential abuse of this information. Those participants who had been less inclined than most to trust the market on security issues found more comfortable ground on privacy, because few participants seemed to feel that the market will prioritize personal privacy.

The discussion of privacy protection was less extensive than some other topics covered during the workshop. Opinions were split on whether new privacy legislation and/or a privacy commission was desirable. There was a general feeling that individuals should be protected from abuses incurred by access to their personal data (e.g., transactional data or "data shadows" that could be reused or sold like a subscribers list), but many were concerned about limiting business opportunities through new controls.

Some participants pointed out that the globalization of the information infrastructure will increase consumer privacy concerns and present security questions (e.g., nonrepudiation of transactions) in home-based applications. One participant recommended a close reading of the Canadian privacy policy as a possible guide for our government.[3] The concepts of a Privacy Commission or a privacy "Bill of Rights" were also brought up as omnibus solutions, but specifics regarding how they might protect personal privacy were not examined.

One of the umbrella points of the privacy debate that most participants agreed to is the need for a "trusted" infrastructure capable of supporting global transactions and trade based on a firm set of ground rules and fair information practices. This trusted infrastructure must support authentication and allow secure transactions. To be implemented such an infrastructure will have to resolve liability[4] and conditional access issues and develop a system of certification controls. Today, differences between the levels of privacy protection in the United States and those of its trading partners, which in general protect privacy more rigorously, could also inhibit development of this infrastructure.

Some participants felt that the common rules of the road for a trusted infrastructure could be the responsibility of a U.S. Privacy Commission. Many of these felt that a close look at the European privacy system would be helpful in establishing guidelines (being the "last ones on the block" to open a Privacy Commission, the United States should not try to set the standard, but should build on the European Union model). Unfortunately, one participant noted, this is a 20-year-old discussion, and as much as industry would like a common set of rules with the European Union, he felt that it is unlikely they will get it in the near future.

Proprietary Information and Intellectual Property

A major concern raised by industry participants was the need to protect intellectual property and proprietary information in electronic form. Companies need to protect their information and transmit it to business partners and offices here and abroad. In light of what many perceived as a growing problem, several individuals recommended a reexamination of "information rights" (e.g., intellectual property rights, confidentiality for proprietary information) in light of the recent changes in information storage and data collection methods

---

[3] See Industry Canada, *Privacy and the Canadian Information Highway* (Ottawa, Ontario: Minister of Supply and Services Canada, 1994), available by WWW from http://debra.dgbt.doc.ca/isc/isc.html. See also Canadian Standards Association, "Model Code for the Protection of Personal Information," CAN/CSA-Q830-1994, draft, November 1994.

[4] For a discussion, see Michael S. Baum, *Federal Certification Authority Liability and Policy,* NIST-GCR-94-654, NTIS Doc. No. PB94-191-202 (Springfield, VA: National Technical Information Service, 1994).

that allow information to be readily copied, aggregated, and manipulated.

Some participants felt that confidentiality of company information could be adequately addressed with better corporate security policies. For example, it may be more difficult to prosecute (or deter) an intruder if a company's log-on screen says "Welcome to Company X" instead of providing a clear statement to inform individuals of the company's intent to prosecute if information on the system is misused or accessed without authorization.

Several participants raised the issue of "corporate privacy" regarding to information not protected by intellectual property laws. Many felt corporations need legal protection for "private" information—that is, information that is proprietary to the corporation, but does not qualify for protection under copyright, patent, or trade secret laws.[5] Though some privacy advocates balk at the concept of "corporate privacy,"[6] several participants felt that a set of standards protecting research and other proprietary information were important to both information security and continued product development. The issue of "corporate privacy" was also raised regarding legal discovery. A few individuals expressed concern over the expense corporations face complying with discovery motions during litigation (e.g., with respect to email and electronic records), but this topic was not explored at length during the day's discussion.

Patent issues and confidentiality of lab documents were of major concern to individuals involved in research and development. They saw a need for evidentiary rules in electronic environments to prevent research fraud, to ensure that electronic lab notebooks are a permanent, enforceable record, and to prosecute intruders.

There was some discussion regarding whether new laws are needed to protect information resources from computer crime—or whether better enforcement is the solution. Some felt that the legal system is not in tune with the new world of computer crime; a world where the computer is the instrument not the target of the crime. Some also felt that the legal profession may not be familiar with "authentication" in electronic environments. Others felt that enforcement is the problem, not the laws. This topic was not examined at length and no consensus was reached.

The question of liability standards for a company in possession of personal data was brought up as an issue in need of a solution. One participant made an urgent plea for a rapid definition of basic legal requirements, to prevent costly retrofitting to meet security and privacy requirements that could be imposed later on. Some believe there should be true and active participation at the federal, state, and local levels to develop consensus on new principles of "fair information practices"[7] that would take into account the ways businesses operate and be flexible enough to meet the needs

---

[5] George B Trubow, *Whether and Whither Corporate Privacy,* essay based on an article prepared for the "DataLaw Report" Gtrubow@jmls.edu.

[6] "The scope of these laws should be limited to the protection of the privacy of personal information; they should not be extended to cover legal persons. Issues relating to companies, such as providing adequate protection for corporate proprietary information, are different and should be the subject of a different body of law." (Business Roundtable, "Statement on Transborder Data Flow—on Privacy and Data Protection," in L. Richard Fischer (ed.), *The Law of Financial Privacy, A Compliance Guide*, 2nd Ed. (New York, NY: Warren, Gorham & Lamont, 1991), appendix 6.3, p. 6-93.)

[7] For example, the Privacy Act of 1974 (Public Law 93-579) embodied principles of fair information practices set forth in *Computers and the Rights of Citizens*, a report published in 1973 by the former U.S. Department of Health, Education, and Welfare. Those principles included the requirement that individuals be able to discover what personal information is recorded about them and how it is used, as well as be able to correct or amend information about themselves. Other principles included the requirement that organizations assure the reliability of personal data for its intended use and take reasonable precautions to prevent misuse. The Privacy Act is limited to government information collection and use. It approaches privacy issues on an agency-by-agency basis and arguably does not address today's increased computerization and linkage of information. See OTA, op. cit., footnote 1, ch. 3.

of various types of individuals and organizations, but that would also offer some stability (or, "safe havens") for new lines of business by delineating acceptable forms of information collection and use. Others did not see a need for omnibus privacy codes or legislation, preferring to deal with problems on an industry-by-industry basis.

As part of the question of liability, it was noted that the tension between network providers and users continues to be unresolved. The dilemma exists between the network providers' inability to monitor content (e.g., invasion of privacy), while at the same time being held responsible for the content of material transferred over their services. One suggestion was to treat network providers more like public utilities and less like publishers.

Views on Congressional Action

This section outlines suggestions made for government action, particularly by Congress. It does not represent the consensus of the participants at the workshop; it only isolates areas that were discussed and lists possible solutions generated during the discussion.

Cryptography Policy and Export Controls

A near consensus was reached regarding the EES (Clipper chip). The vast majority felt that it was poorly handled, poorly conceived, and did not take into account the structure of today's world economy. It is a national standard in an international economy. It will exacerbate the problems with export controls, by having one system (EES) in the United States and one system (DES or another system) outside the United States. Many felt that it is an enormous distraction that, coupled with export controls, will allow foreign countries to get ahead of us in the global information infrastructure.

Several participants felt that the United States is getting out of step with the international community, and appears pointed in the wrong direction on information security. Many industry representatives feel that the potential of U.S. policies to damage the economy and U.S. industry is not being given priority by the people making decisions.

Possible Congressional Actions:

- Review export controls and find a feasible middle ground.
- Review the executive decision on the Clipper chip.
- Promote consumer use of a public-key infrastructure.
- Open up a public dialogue with NIST, the National Security Agency (NSA), and the Federal Bureau of Investigation (FBI) on the international availability of cryptography.
- State that the international competitiveness of the United States in information systems and communications is a priority in considering cryptography policy.

Federal Standards and Open Dialogue

There was a general consensus on the need for ground rules and standards for safeguarding information, but much disagreement on how this should be done. There was sentiment that leadership is needed from the government on these issues. However, many participants did not think the government should or could set these standards. 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 introduction of the Clipper chip and promulgation of the EES, is 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. Several individuals felt that dialogue on information policy is paralyzed because NSA is not allowing open discussion nor responding in any tangible way to the needs of industry. Many par-

ticipants 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 Computer Systems Security and Privacy Board (CSSPAB) was suggested as one stimulus for generating dialogue between industry and government, but according to several participants the committee is not well utilized. In addition, there exists an information gap: the CSSPAB was "kept in the dark" about the Clipper initiative, then after it gathered information through public meetings, the information and CSSPAB recommendations were ignored by the Commerce Department.

Possible Congressional Actions:

- Define basic legal requirements to prevent unnecessary and retroactive security measures.
- Revise the export administration act in order to allow multinationals to set up ubiquitous security standards through U.S. vendors.
- Increase oversight of the Computer Security Act as it relates to the relationship between NSA and NIST and review the Memorandum of Understanding between NSA and NIST. Encourage more open dialogue with and utilization of the CSSPAB.
- Encourage NIST to develop a Certification Standard to support interoperability across networks, rather than picking technological standards.
- Redefine national security priorities.

Information Security in Federal Agencies

Participants suggested that there needs to be more emphasis on securing unclassified information and that there needs to be leadership. According to some participants: the government should get "its house in order" in the civilian agencies; few companies are so badly managed as government agencies; senior managers are unaware of responsibilities and untrained. As a result, participants noted, 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 there has been overemphasis on cryptography, to the exclusion of management; severe problems like errors and dishonest employees are not addressed by this "technology" focus. Participants considered that the real issue is *management*; technology sloganism along the lines of "buy C2 [a computer security rating] and you're OK" is not enough. 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 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.

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 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.

Possible Congressional Actions:

- Implement oversight of the Computer Security Act with special attention to management of information-security policy.
- Fully fund NIST so it can "sort out the 'tower of Babel' in cryptographic capabilities and system interoperability." Several participants sug-

gested trying to encourage better standards policy by using the General Accounting Office to audit agency compliance with NIST standards, or mandating that agencies respond to CSSPAB recommendations.
- Encourage more attention to management practices. Review OMB Circular A-130 with particular emphasis on implementation.

Privacy

The privacy issue in general came up often, but no one had a detailed solution. There is an urgent sense that something needs to be done, because questions of personal privacy and "corporate privacy" continue to cause controversy and the problems will only increase as network access expands. The only concrete suggestion, which was not universally endorsed, is the creation of a Privacy Commission, possibly with a cabinet-level head or as a part of the Commerce Department.

One frequently mentioned topic was for government recognition of U.S. industry's need for consistency between U.S. privacy laws and European privacy laws. This reflects the industry orientation toward the international nature of the economy.

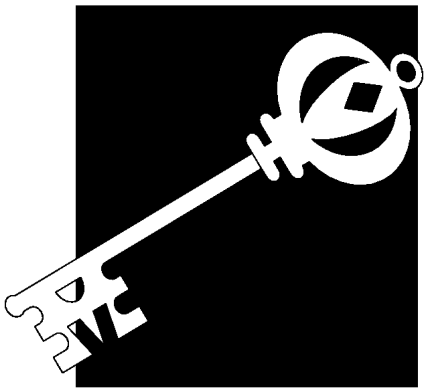
Several participants called on Congress to review liability issues and intellectual-property concerns, with respect to electronic information and networks. Some participants felt the need to protect providers from action taken over their networks. Some suggested that network providers be treated more like a public utility, removed from liability for the content of the material carried over their networks.

Possible Congressional Actions:
- Establish a Privacy Commission.
- Determine regulatory status and liability of network providers.
- Review intellectual-property laws for enforcement in electronic environments.
- Examine European Union privacy laws and review the possibility of bringing U.S. privacy protections closer to theirs.

Implications for Congressional Action 4

Since the 1994 OTA report *Information Security and Privacy in Network Environments*[1] was published, security concerns like "sniffing" and "spoofing" by intruders, security holes in popular World Wide Web software, and intrusions into commercial and government networks have continued to receive attention:

- Password sniffers capture legitimate users' passwords for later use by intruders. Spoofing involves the use of fake origination addresses, so that an incoming connection will appear to come from somewhere else, usually a "legitimate" or "trusted" Internet network protocol (IP) address.[2]
- The U.S. Department of Energy's computer security response group alerted Internet users to, and issued corrections for, a flaw in a version of the free UNIX software commonly used to create World Wide Web "home pages." Depending on how a World Wide Web server is configured, the vulnerability could permit a hacker to access the computer's main, or "root" directory. Commercial Web products under development (e.g., for



[1] 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). See *Congressional Record*, Sept. 22, 1994, pp. S13312-13 (statement of Senator William V. Roth, Jr. announcing release of the OTA report).

[2] See Michael Neubarth et al., "Internet Security" (special section), *Internet World*, February 1995, pp. 31-72. See also William Stallings, *Network and Internetwork Security: Principles and Practice* (Englewood Cliffs, NJ: Prentice Hall (IEEE Press), 1995, chapter 6.

electronic commerce) are incorporating additional security features.[3]

- During 1993-94, the Defense Information Systems Agency (DISA) conducted mock attacks on 8,932 Defense Department computers. The DISA team broke into 7,860 of these, but the systems' computer administrators detected only 390 of the successful "sting" intrusions. Only about 20 reported the incident. DISA estimates that real attacks on Defense systems average about one per day.[4]

The increasing prominence of the Defense Department's "Information Warfare" doctrine is raising awareness of threats from economic espionage, global organized crime, and terrorism.[5] Awareness of technical countermeasures like *firewalls*, active intrusion-detection systems, one-time password generators, and challenge-response user authentication systems[6] continues to rise, although use lags for a number of reasons, including cost.[7]

This chapter provides an update of 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. It also discusses the most recent attempts within the executive branch to centralize unclassified-information-security authorities government-wide. The proposed "new order" presented in the Security Policy Board staff's 1994 report (see below) would increase the government-wide authorities of the defense and intelligence agencies for unclassified information security within the federal government. Such an expansion of authorities would run counter to the unclassified-information-security structure mandated by the Computer Security Act of 1987 (see chapter 2 and appendix B), as well as the agency responsibilities set forth in the Paperwork Reduction Act of 1995 (see below) and the new, proposed revision to Appendix III of OMB Circular A-130 (see below). The chapter concludes with a discussion of the implications of these developments for congressional consideration of issues and options identified in the 1994 OTA report *Information Security and Privacy in Network Environments.*

UPDATE ON CRYPTOGRAPHY INITIATIVES

This section highlights selected government and commercial cryptography developments since publication of the 1994 report. This is not a comprehensive survey of commercial information-security products and proposals. Mention of individual companies or products is for illustrative purposes and/or identification only, and

---

[3] See Elizabeth Sikorovsky, "Energy Group Uncovers Hole in Web Software," *Federal Computer Week*, Feb. 20, 1995, pp. 3-4; and Richard W. Wiggins, "Business Browser," *Internet World*, February 1995, pp. 52-55.

[4] See, e.g., Jared Sandberg, "GE Says Computers Linked to Internet Were Infiltrated," *The Wall Street Journal*, Nov. 28, 1994; or Bob Brewin and Elizabeth Sikorovsky, "DISA Stings Uncover Computer Security Flaws," *Federal Computer Week*, Feb. 6, 1995, pp. 1-45. See also Vanessa Jo Grimm, "In War on System Intruders, DISA Calls in Big Guns," *Government Computer News*, Feb. 6, 1995, pp. 41-42.

[5] See Neil Munro, "New Info-War Doctrine Poses Risks, Gains," *Washington Technology*, Dec. 22, 1994, pp. 1, 12; and "How Private Is Your Data?" *Washington Technology*, Feb. 9, 1995, pp. 14, 16.

[6] *Firewalls* are network barriers that filter network traffic, for example, denying incoming telnet or ftp connections except to designated directories, from designated network domains or IP addresses. Active intrusion-detection systems look for anomalous or abnormal processes (like extended log-on attempts as an intruder tries to "guess" valid passwords, attempts to copy password files or system programs), curtail them, and alert security officers. See, e.g., Stallings, op. cit., footnote 2; Warwick Ford, *Computer Communications Security* (Englewood Cliffs, NJ: Prentice Hall, 1994); and Jeffrey I. Schiller, "Secure Distributed Computing," *Scientific American*, November 1994, pp. 72-76.

[7] Recent government efforts to promote use of security technologies include several cataloging and technology transfer efforts undertaken by the Office of Management and Budget, National Institute of Standards and Technology, and the Defense Department. See Neil Munro, "Feds May Share Security Tech," *Washington Technology*, Nov. 10, 1994, pp. 1, 22.

should not be interpreted as endorsement of these products or approaches.

Executive Branch Developments[8]

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.[9] However, there has been no formal commitment to eventually adopting any alternative to Skipjack in a federal escrowed-encryption standard for computer data.[10] Moreover, there has been no commitment to consider alternatives to the EES for telephony.

The question of whether or when there will be key-escrow encryption federal information processing standards (FIPS) for unclassified data communications and/or file encryption is still open. There is at present no FIPS specifying use of Skipjack for these applications. (The EES specifies an implementation of Skipjack as a standard for use in telephone, not computer, communications.) However, the Capstone chip and FORTEZZA card implementation of the Skipjack algorithm is being used by the Defense Department in the Defense Message System.

Furthermore, there has been no backing away from the underlying Clinton Administration commitment to "escrowing" encryption keys. With escrowing, there is mandatory key deposit. In the future, there may be some choice of "escrow agencies" or registries, but at present, EES and Capstone-chip keys are being escrowed within the Commerce and Treasury Departments. The notion of optional deposit of keys with registries, which OTA referred to 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), is not being considered.[11]

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). At present, there is no FIPS for secure key exchange (e.g., for use with the Data Encryption Standard (DES).

Turning from encryption to digital signatures, acceptance and use of the new FIPS for digital signatures are progressing, but slowly. As the 1994 report detailed in its description of the evolution of the Digital Signature Standard (DSS), patent problems complicated the development and promulgation of the standard.[12] 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 in-

---

[8] See also OTA, op. cit., footnote 1, pp. 171-182.

[9] For background, see appendix E of this background paper and OTA, op. cit., footnote 1, pp. 15-16 and 171-174. The Escrowed Encryption Standard is described in box 2-3 of this background paper.

[10] 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 (DSS—see box 2-2) and key-exchange functions.

[11] See OTA, op. cit., footnote 1, p. 171.

[12] See OTA, op. cit., footnote 1, appendix C, especially pp. 220-21. For a more recent account of the various lawsuits and countersuits among patentholders, licensers, and licensees, see Simson Garfinkle, *PGP: Pretty Good Privacy* (Sebastopol, CA: O'Reilly and Assoc., 1995), esp. ch. 6.

demnify vendors that develop certificate authorities for a public-key infrastructure.[13]

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 Digital Signature Standard (DSS). For example, some federal agencies (e.g., the Central Intelligence Agency) have already purchased and implemented commercial software packages containing RSA-based security features.[14] Moreover, many agencies and their contractors are interested in software-based signature systems, rather than hardware-based implementations. For example, the Westinghouse Savannah River Company, which is the management and operating contractor for the DOE at the Savannah River Site, is seeking a business partner under a cooperative research and development agreement (CRADA) arrangement for collaborative development of software involving application and integration of the DSS into business-applications software packages. The goal of the CRADA project is to produce a software product or module that can be used to replace paper-based approval signatures with digital signatures. These digital signatures would be used, for example, for time and attendance reporting, travel expense reporting, and other forms management and routing in local area networks.[15]

Cost, as well as interoperability with the private sector, is an issue. The DSS can be implemented in hardware, software, or firmware, but the National Security Agency's (NSA's) preferred implementation is in the FORTEZZA card, along with the EES algorithm. The FORTEZZA card (formerly called the TESSERA card) is a Personal Computer Memory Card Industry Association (PCMCIA) card.[16] 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 Department's 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 NSA, unit costs should be below the $100 per unit target established for the program.[17] Thus, the FORTEZZA production

---

[13] 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 1, ch. 3.

[14] See Brad Bass, "Federal Encryption Policy Shifts Direction," *Federal Computer Week*, Feb. 20, 1995, pp. 28-29. Lotus Notes [TM], a "groupware" package that has RSA public-key and access-control security features, is reportedly used to handle over 85 percent of the Central Intelligence Agency's (CIA's) email traffic. (Adam Gaffin, "CIA Espies Value in Turning to Lotus Notes," *Network World*, Mar. 13, 1995, p. 43.)

[15] *Commerce Business Daily*, Apr. 5, 1995.

[16] 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.

[17] 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.).

contract would be on the order of $20 million to $40 million.

The National Institute of Standards and Technology (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, pp. 20 and 164).

Due to lack of procurement funds and to avoid duplicating other agencies' operational efforts, NIST did not issue a solicitation for public-key certificate services. The U.S. Postal Service and the General Services Administration have at present taken the lead on a government public-key infrastructure.[18] The 1996 Clinton Administration budget proposals reportedly do not specify funds for NIST work related to the DSS, or the EES.[19] 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 (PKI) 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, 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 JTO will be to:

- Encourage the U.S. industrial base to develop commercial products with built-in security to be used in Defense Department 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 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.[20]

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

---

[18] F. Lynn McNulty et al., NIST, personal communication, Feb. 24, 1995.

[19] 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.

[20] "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).

Private Sector Developments

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.[21] 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.[22] 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. These 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 (ASC X9), which sets data security standards for the U.S. banking and financial services industries, has announced that it will develop new encryption standards based on triple DES. ASC X9 will designate a subcommittee to develop technical standards for triple-DES applications.[23]

RSA Data Security, Inc., recently announced another symmetric encryption algorithm, called RC5.[24] 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), from the same company, is a 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.[25]

Another private sector standards group, the IEEE P1363 working group on public-key cryptography, is developing a voluntary standard for "RSA, Diffie-Hellman, and Related Public-Key Cryptography" (see figure 2-5). The group held a public meeting in Oakland, California, on May 10, 1995, to review a draft standard.[26]

Several companies and individuals have proposed alternative approaches to key-escrow encryption.[27] According to a "taxonomy" by Dorothy Denning and Dennis Branstad, there are some 20 different alternatives, including:

---

[21] 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.

[22] 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.

[23] *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).

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

[25] 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.

[26] 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>.

[27] See Elizabeth Corcoran, "Three Ways To Catch a Code," *Washington Post*, Mar. 16, 1995, pp. B1, B12. The article also discusses the Hewlett-Packard's proposed "national flag card" approach to government-approved encryption.

- AT&T CryptoBackup,
- Bankers Trust International Corporate Key Escrow,
- Bell Atlantic Key Escrow,
- Fortress KISS,
- Micali Fair Cryptosystems,
- TECSEC VEIL,
- TIS Commercial Software Key Escrow System,
- and
- TIS Software Key Escrow System.[28]

Variously, these use public (i.e., published, unclassified) encryption algorithms, thus potentially allowing implementation in software as well as hardware. They use commercial or private key-escrow systems, with data recovery services that can be made available to individuals and organizations, as well as to law enforcement (with proper authorization). A brief description of two of the commercial approaches follows, 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. According to Bankers Trust, its international private key-escrow system ensures privacy and security, while preserving law enforcement and national security capabilities. Bankers Trust believes there is a need for escrowed keys in business applications, so that encrypted information can be recovered when a key has been lost or is otherwise unavailable. The Bankers Trust system supports different encryption methods, thus accommodating different national policies (e.g., regarding export, import, or use controls). The Bankers Trust system uses a hardware device to encrypt information stored in and transmitted through global information infrastructures, including voice, fax, store-and-forward messaging, and data-storage-and-retrieval systems. Bankers Trust believes that the requirement of a device will be consistent with the rapidly emerging use of smart cards for network financial transactions, together with the need to secure the global information infrastructure against potential abuse.[29]

Under Bankers Trust's system, the owner of the encryption device selects an encryption algorithm and escrows the key or fragments of the key with one or more trusted entities (escrow agents). These could be a commercial company. The system allows owners to freely change algorithms, keys, and agents at any time; owners might make these changes as part of a standard security policy or as an added security measure after any suspected problem. Bankers Trust's system enables owners to access their key(s) to decrypt encrypted information when necessary. It also permits law enforcement, with proper legal authorization, to obtain keys to decrypt information. Additionally, it contains extensive audit and other procedures to ensure the integrity of the system.[30]

The government is looking at various alternative approaches to key-escrow encryption. At this writing, the commercial escrowing alternative proposed by Trusted Information Systems, Inc., is undergoing internal government review to determine whether such an approach may be feasible to meet national security and law enforcement objectives.[31] The TIS approach is software rather than hardware-based.[32] Like the Bankers Trust system, but in contrast to the EES/Capstone approach to escrowing, it would also permit the rightful "key

---

[28] See Dorothy E. Denning and Dennis Branstad, "A Taxonomy for Key Escrow Encryption," forthcoming, obtained from the author (denning@cs.georgetown.edu).

[29] Nanette DiTosto, Bankers Trust, personal communication, Apr. 10, 1995.

[30] Ibid.

[31] F. Lynn McNulty, Associate Director for Computer Security, NIST, personal communications, Feb. 24, 1995 and Mar. 21, 1995.

[32] Stephen T. Walker, et al., "Commercial Key Escrow: Something for Everyone, Now and for the Future," Jan. 3, 1995, Trusted Information Systems, Inc., TIS Report No. 541.

owners"—not just law enforcement agencies—to recover the contents of encrypted messages or files, if the keys became unavailable due to accident, malfeasance, error, or so forth.

In the TIS scheme, a user would register his or her escrowed-encryption computer program with a commercial, government, or corporate data recovery center. The interactive registration process would provide the user's computer program with information to be used in creating the "data recovery field" (analogous to the LEAF in the EES method—see box 2-3) that would be appended to all encrypted communications (or files). Any encryption algorithm could be used but the software implementation cannot protect the "secrecy" of a classified algorithm. According to TIS, its proposal relies on "binding" a software key-escrow system to the chosen encryption algorithm. Implementing this type of software "binding" is difficult, but if done properly, it would prevent someone from separating the computer program's encryption functions from the key-escrowing functions and would prevent use of the program for encryption using nonescrowed keys. The "binding" features of the TIS proposal are intended to prevent use of the encryption function if key escrowing is disabled, or "spoofing" the system by creating spurious data recovery fields.[33]

UPDATE ON BUSINESS PERSPECTIVES

Representatives of major U.S. computer and software companies have reaffirmed the importance of security and privacy protections in the developing *global* information infrastructure (GII). According to the Computer Systems Policy Project (CSPP):

> The GII will not flourish without effective security mechanisms to protect commercial transactions. Consumers and providers of products and services, particularly those involving health care and international commerce, will not use GII applications unless they are confident that electronic communications and transactions will be confidential, that the origin of messages can be verified, that personal privacy can be protected, and that security mechanisms will not impede the transnational flow of electronic data.[34]

But 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:

> Governments have a critical interest in commercial security mechanisms that are consistent with their own national security needs. As a result, they must participate in private sector efforts to develop and adopt security standards. However, government needs should not be used as reasons to replace or overwhelm the private sector standards processes.

To meet the security goals for the GII (as well as privacy goals supported by security solutions), the CSPP recommended that:

- All participating countries must adopt standards to support mechanisms that are acceptable to the private sector and suitable to commercial transactions. These standards must also ensure privacy and authentication. This may require nations to adopt commercial security solutions that are different and separate from solutions for national security and diplomatic purposes.
- The U.S. government must cooperate with industry to resolve U.S. policy concerns that have blocked acceptance of international encryption mechanisms necessary for commercial transactions.
- The private sector and government should convene a joint international conference to address the need for security mechanisms to support commercial applications and to de-

---

[33] Steve Lipner, Trusted Information Systems, Inc., personal communication, Jan. 9, 1995. According to Lipner, the National Security Agency introduced the term *binding* to the lexicon, to refer to this feature.

[34] Computer Systems Policy Project, *Perspectives on the Global Information Infrastructure*, February 1995, p. 9.

velop a strategy for implementing acceptable security solutions.[35]

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, prepared by a panel drawn from government, the computer industry, and the legal and academic communities, discussed the history and technology of cryptography and the value and importance of privacy, concluding with identification of 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?[36]

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 future users of the National Information Infrastructure (NII).[37]

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."[38] 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:

- Different encryption methods will be needed to fulfill a variety of user needs. Users should be free to use and implement the already existing framework of generally available and generally accepted encryption methods and to choose keys and key management without restrictions. Cryptographic algorithms and key-management schemes must be open to public scrutiny for the commercial sector to gain the necessary level of confidence in them.
- Commercial users, vendors, and governments should work together in an open international forum in preparing and approving global standards.

---

[35] Ibid., pp. 9-10.

[36] Susan Landau et al., "Codes, Keys, and Conflicts: Issues in U.S. Crypto Policy," Association for Computing Machinery, Inc., June 1994.

[37] USACM, June 1994.

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

- Both hardware and software implementations of encryption methods should be allowed. Vendors and users should be free to make technical and economic choices about modes of implementation and operation.
- Owners, providers, and users of encryption methods should agree on the responsibility, accountability, and liability for such methods.
- With the exception of encryption methods specifically developed for military or diplomatic uses, encryption methods should not be subject to export or import controls, usage restrictions, restrictive licensing arrangements, or other restrictions.[39]

The United States Council for International Business (USCIB) subsequently issued position papers on "Business Requirements for Encryption"[40] and "Liability Issues and the U.S. Administration's Encryption Initiatives."[41] 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, flexibility in implementation (hardware or software), and liability requirements for escrow agents if escrowing is used:

> Business recommends the removal of unfounded export controls on commercial encryption. In the absence of relief from export controls, business recommends that the following steps be undertaken in order to achieve an encryption policy that is internationally acceptable:
>
> (a) the Administration endorse the requirements outlined in this paper
> (b) the Administration enter into bilateral and multilateral discussions with other nations to achieve the widespread adoption of these requirements.

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.[42]

The USCIB has also identified a number of distinctive business concerns with respect to 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 tamperproof 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 connection with the EES and Capstone initia-

---

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

[40] United States Council for International Business, "Business Requirements for Encryption," New York, NY, Oct. 10, 1994.

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

[42] USCIB, op. cit., footnote 40, pp. 3-4.

tives, 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.[43]

These types of concerns have remained unresolved (see related discussion and options presented in the 1994 OTA report, pp. 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.[44]

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.[45]

The Utah Digital Signature Act[46] is intended to provide a reliable means for signing computer-based documents and legal recognition of digital signatures using "strong authentication techniques" based on asymmetric cryptography. To assure a minimum level of reliability in digital signatures, the Utah statute provides for the licensing and regulation of certification authorities by a "Digital Signature Agency" (e.g., the Division of Corporations and Commercial Code of the Utah Department of Commerce). The act, first drafted as a proposed model law, provides that the private key is the property of the subscriber who rightfully holds it (and who has a duty to keep it confidential); thus, tort or criminal actions are possible for theft or misuse. It is technology-independent; that is, it does not mandate use of a specific signature technique.[47] The management of the system described in the Utah statute can easily

---

[43] USCIB, op. cit., footnote 41, pp. 2-6.

[44] See footnote 13 for discussion of liability exposure, legal considerations, tort and contract remedies, government consent to be liable, and recommendations and approaches to mitigate liability.

[45] Information on the 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).

[46] Utah Digital Signature Legislative Facilitation Committee, "Utah Digital Signature Legislation," Dec. 21, 1994. The Utah Digital Signature Act was signed into law on March 10, 1995, as section 46-3-101 et seq., *Utah Code Annotated*. (Prof. Lee Hollaar, University of Utah, personal communication, Mar. 22, 1995.)

[47] Utah Digital Signature Act, ibid. The model legislation was endorsed by the American Bar Association, Information Security Committee of the Science and Technology Section, EDI/Information Technology Division; Prof. Lee Hollaar, University of Utah; Salt Lake Legal Defenders Assoc.; Statewide Association of Public Attorneys; Utah Attorney General's Office; Utah Dept. of Corrections; Utah Information Technology Commission; Utah Judicial Council; and Utah State Tax Commission.

be privatized and globalized.[48] The information at the Digital Signature Agency can be as little as the authorization of one or more private sector certificate authorities; a certificate authority can operate in many states, having authorizations for each.[49]

UPDATE ON 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 legislation (H.R. 184) to establish a Privacy Protection Commission.

The "Individual Privacy Protection Act of 1995" (H.R. 184) is identical to legislation Representative Collins introduced in the 103rd Congress (H.R. 135). Both bills are similar to legislation introduced in the 103rd Congress by Senator Paul Simon (S. 1735). The establishment of a Privacy Protection Commission was endorsed by the Vice President's National Performance Review and encouraged in a 1993 statement by Sally Katzen, the Administrator of the Office of Information and Regulatory Affairs in the Office of Management and Budget.[50] H.R. 184 would establish a five-member 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, 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.[51] Some have raised concerns about the bill on the grounds that it might danger-

---

[48] The Utah act envisions use of signatures based on standards similar to or including the ANSI X.9.30 or ITU X.509 standards (ibid.).

[49] Prof. Lee Hollaar, University of Utah, personal communication, Mar. 22, 1995.

[50] Statement by Sally Katzen, Administrator, Office of Information and Regulatory Affairs, OMB and Chair, Information Policy Committee, Information Infrastructure Task Force, Nov. 18th, 1993 (*Congressional Record*, p. S.5131).

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

ously limit local police authority to question minors and threaten investigations of child abuse, or hinder doctors in obtaining timely patient information on children.[52]

In addition, the Office of Management and Budget recently published notice of "Draft Principles for Providing and using Personal Information and Commentary.[53]" These 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 that was developed in the early 1970s and used in development of the Privacy Act of 1974.

UPDATE ON 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. There are a variety of Information Warfare activities ongoing in Department services and agencies, the Office of the Secretary of Defense, and elsewhere.[54] The Department's Defensive Information Warfare program goals focus on technology development to counter vulnerabilities stemming from its 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 increasing 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.
>
> 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.[55]

Such a consolidation and/or expansion would run counter to current statutory authorities and to the Office of Management and Budget the Office of Management and Budget (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."[56] The Joint Security Commission's report made recommendations across a comprehensive range of areas, including:

- classification management;
- threat assessments;
- personnel security and the clearance process;
- physical, technical, and procedural security;
- protection of advanced technologies;
- a joint investigative service;
- accounting for the costs of security;

---

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

[53] *Federal Register*, Jan. 20, 1995, pp. 4362-4370.

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

[55] Ibid., p. 52.

[56] 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.

- security awareness, training, and education;
- information systems security; and
- a security architecture for the future [emphasis added].[57]

The Joint Security Commission report's sections on information systems security[58] and a security architecture for the future[59] are of special interest. In the context of its charter, the Commission proposes a unified security policy structure and authority for classified and unclassified information in the defense/intelligence community.[60] However, the report also recommends a more general centralization of information security along these lines government-wide; the executive summary highlights the conclusion that the security centralization within the defense/intelligence community described in the report should be extended government-wide.[61] 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."[62]

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.[63] 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 OMB and NSC staff.

The Security Policy Forum that had been established under the Joint Security Executive Committee 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.[64]

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"

---

[57] Joint Security Commission, ibid.

[58] Ibid., pp. 101-113.

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

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

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

[62] Ibid., p. 130.

[63] 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.

[64] Ibid. (fact sheet).

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."[65] 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 Board's staff 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 SPB 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.[66]

The SPB staff report's proposed "new order" for information security builds on the Joint Security Commission's analysis and recommendations to establish a "unifying body" government-wide.[67] 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." The SPB staff report generally notes that:

> Realignment into this new structure will require a transition effort that will include the necessary coordination to effect changes to several executive and legislative edicts.
>
> . . . An endorsement of this proposed reorganization will include authorization for the Director, Board Staff to proceed with the establishment of a transition team and coordinate all activities necessary to effect the U.S. Government's conversion to this new structure.[68]

As motivation for the changes, the SPB staff report notes that:

> Nowhere in the proposed new order does the goal to create cohesive, cost-effective, and operationally effective security policy encounter a greater challenge than in the area of protecting information systems and networks. The national architecture under development will provide vast amounts of information to all consumers rapidly and for a reasonable price. The ability to link and communicate with a wide variety of networks will not only be a key to productivity but will also be an "Achilles heel." Some of this nation's most significant vulnerabilities lie within the sensitive but unclassified networks that perform the basic function that we all take for granted. The coupling of policy requirements for sensitive but unclassified systems within those for classified systems dictates the need for a comprehensive structure to address these needs in a cohesive fashion.[69]

This "comprehensive structure" would be the new Information Systems Security Committee (ISSC), which would be:

---

[65] Ibid.

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

[67] 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.

[68] U.S. Security Policy Board Staff , op. cit., footnote 66, p. II-III.

[69] Ibid., p. 15.

> . . .based on the foundation of the current NSTISSC [National Security Telecommunications and Information Systems Security Committee, see appendix B] 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 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 [Information Security] 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 unclassified arena from a national security standpoint* [emphasis added]. Issues such as voting in such a potentially unwieldy organization must also be resolved.[70]

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, the proposals have been met with concern and dismay reminiscent of reactions to National Security Decision Directive-145 (NSDD-145) a decade ago (see chapter 2 and appendix B).[71] 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 those 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 government-wide 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."[72]

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, Administrator, Office of Information and Regulatory

---

[70] Ibid., pp. 17-18. See appendix C of this paper and OTA, op. cit., footnote 1, pp. 132-148 for discussion of NSDD-145, the intent of the Computer Security Act of 1987, and NSTISSC.

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

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

Affairs (released March 23, 1995), the Steering Committee of the Federal Computer Security Program Manager's Forum[73] indicated "unanimous disagreement" with the Security Policy Board's proposal and urged OMB to "take appropriate action to restrict implementation of the SPB report to only classified systems" for the following reasons:

1. The establishment of a national security community dominated Information System Security Committee having jurisdiction for both classified and unclassified systems is contrary to the Computer Security Act. Furthermore, it is not consistent with the authority of PDD-29 which requires coordination of national security policy [emphasis added].
2. This initiative also undercuts a stated Administration goal for an "open government" in which the free flow of information is facilitated by removing government restrictions and regulations. For example, the SPB document states that a priority project for the new committee will be to craft a broad new definition for "national security related information." This will be viewed by many as an attempt to impose new restrictions on access to government information.
3. The SPB proposal may serve to increase concerns over the government's intentions in the field of information security. We know from observing the public debate over NSDD-145 and the Clipper Chip that the private sector deeply mistrusts the intentions of the government to use information security policy as a lever to further goals and objectives viewed as contrary to the interests of the business community. Congress passed the Computer Security Act of 1987 in response to expressions of displeasure from the private sector regarding the unwelcome overtures by the national security community towards "assisting" the private sector under the auspices of national security. This was perceived as having a significant adverse impact upon personal privacy, competitiveness and potential trade markets.
4. We believe that it is inappropriate for the national security and intelligence communities to participate in selecting security measures for unclassified systems at civilian agencies. Their expertise in protecting national security systems is not readily transferable to civil agency requirements. The primary focus of security in the classified arena is directed towards protecting the confidentiality of information with little concern for cost effectiveness. Unclassified systems, however, which constitute over 90% of the government's IT [information technology] assets, have significantly fewer requirements for confidentiality vis-a-vis the need for integrity and availability. In these times of diminishing resources, cost-effectiveness is of paramount concern in the unclassified arena.[74]

The letter concludes:

> The Steering Committee is most concerned that the report is being misrepresented as Administration policy. Indicative of this is that "transition teams" are being formed to implement the report.
>
> Please consider these facts and take action to restrict the SPB report implementation to only classified systems.[75]

This type of restriction appears to have been incorporated in the proposed revision to Appendix III of OMB Circular A-130 (see below).

---

[73] 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 Jan. 11, 1995, letter to Sally Katzen 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.

[74] Ibid.

[75] 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.[76]" 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 on page 30.

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.[77] The Paperwork Reduction Act of 1995 (Public Law 104-13) was reported on April 3, 1995[78] and passed in both Houses on April 6, 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.[79]

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.

---

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

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

[78] 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 paper.

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

59 note), to 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.[80]

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)).[81]

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.[82]

Proposed Revision of OMB Circular A-130 Appendix III

At this writing, OMB has 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 authority 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.[83]

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

---

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

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

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

[83] 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>.

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.[84] 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.[85]

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.[86]

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]."[87] 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.[88]

Otherwise, the proposed OMB guidance assigns government-wide responsibilities to agencies that are "consistent with the Computer Security Act." These include the Commerce Department, through NIST; the Defense Department, through NSA; the Office of Personnel Management; the General Services Administration, and the Justice Department.[89]

A complete analysis of the proposed revision to Appendix III is beyond the scope of this back-

---

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

[85] Office of Management and Budget, op. cit., footnote 83.

[86] Ibid., p. 4.

[87] Ibid., p. 15.

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

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

ground 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.[90]

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 consider 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

The next sections discuss implications of the above for congressional actions related to cryptography policy and government information security, in the context of issues and options OTA identified in its 1994 report *Information Security and Privacy in Network Environments* (see appendix D of this paper and/or chapter 1 of the 1994 report).

Export Controls and Standards

Reform of the current export controls on cryptography was certainly the number one topic at the 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.[91]

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. 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 Administration's market study, and by encouraging a more timely, open, and productive dialogue between

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

[91] See appendix C, especially footnote 10 and accompanying text.

government and the private sector (see pages 11-13, 150-160, 174-179 of the 1994 OTA report.)

Oversight of the implementation of the Computer Security Act is also important to cryptography policy considerations (see below). The cryptography-related federal information processing standards 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 1994 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.

Finally, 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 escrow agencies for Clipper and Capstone chips and prices and expenditures for the FORTEZZA cards. The latter may be indicative of the likelihood of the "PCMCIA portfolio" FORTEZZA approach finding favor in the civil agencies and in the private sector, compared with more flexible and/or disaggregate implementation of encryption and signature functions.

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 information security and privacy risks incurred in downsizing and the general lack of commitment by 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 on information security and privacy in network environments 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 be 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 *Information Security and Privacy in Network Environments*, 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 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 appendix D and pages 18-20 of the 1994 OTA report), 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 technical assistance) evaluating new information technologies to assess their security vulnerabilities and apprising agencies of these in a timely fashion.[92]

Locus of Authority

Another reason for the importance and timeliness of congressional oversight of government-wide information-security policy guidance is that there is 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's 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/intelligene community—then vigilant oversight and clear direction will be needed to ensure effective implementation, including assigning and funding a credible focal point 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 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 governmentwide 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 1994 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 informa-

[92] OMB, op. cit., footnote 83, p. 7.

tion are for the most part spinoffs from the classified domain;
2. the defense and intelligence agencies are expert in classified information security; and therefore
3. the unclassified domain can best be served by extending the authority of the defense/intelligence agencies.

The validity of the "spinoff" 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 III 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.[93]

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.)

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

Appendix A: Congressional Letter of Request

A

JOHN GLENN, OHIO, CHAIRMAN

SAM NUNN, GEORGIA
CARL LEVIN, MICHIGAN
JIM SASSER, TENNESSEE
DAVID PRYOR, ARKANSAS
JOSEPH I. LIEBERMAN, CONNECTICUT
DANIEL K. AKAKA, HAWAII
BYRON L. DORGAN, NORTH DAKOTA

WILLIAM V. ROTH, JR., DELAWARE
TED STEVENS, ALASKA
WILLIAM S. COHEN, MAINE
THAD COCHRAN, MISSISSIPPI
JOHN McCAIN, ARIZONA
ROBERT F. BENNETT, UTAH

LEONARD WEISS, STAFF DIRECTOR
FRANKLIN G. POLK, MINORITY STAFF DIRECTOR AND CHIEF COUNSEL

United States Senate

COMMITTEE ON
GOVERNMENTAL AFFAIRS
WASHINGTON, DC 20510-6250

October 7, 1994

Dr. Roger C. Herdman
Director
Office of Technology Assessment
United States Congress
Washington, D.C. 20510-8025

Dear Dr. Herdman:

Thank you again for the fine report, Information Security and Privacy In Network Environments. As you may recall, that report was prepared in response to our interest in how government policies must adapt to changes in communications network technologies that affect the privacy and economic livelihood of every American. The report highlights key issues and makes recommendations that should serve as the basis for hearings and legislation. Towards that end, we are writing to ask for your assistance in working with our staff to follow-up and develop further the findings of the report.

We would appreciate it if the project director, Ms. Joan Winston, be provided sufficient staff and resources to assist our staff in preparing for hearings and subsequent legislation. In particular, we request analytical support on policy requirements and alternatives, including further insights in computer network security problems that affect the survivability and reliability of such networks. In addition, the Committee needs information gathered from industry, government agencies, and other sources in response to issues raised in the report, including relevant implications of emerging technology. In carrying out this request, we would also like the Office of Technology Assessment to host a meeting with representatives of industry, government, and academia to discuss the findings of the report.

The Office of Technology Assessment report underscores the fact that much more work must be done. There are many questions about the role of government that the Governmental Affairs Committee must address. We would appreciate your continued cooperation.

Sincerely,

Bill Roth
William V. Roth, Jr.
Ranking Republican Member

John Glenn
John Glenn
Chairman

Appendix B: Federal Information Security and the Computer Security Act

B

This appendix draws on chapter 4 of the September 1994 OTA report *Information Security and Privacy in Network Environments*,[1] with updates as noted herein. That chapter of the 1994 report examined the policy framework within which federal agencies formulate and implement their information-security and privacy policies and guidelines. Because of its importance for federal government information security and cryptography policy, the Computer Security Act of 1987 (Public Law 100-235) was examined in detail.

The Computer Security Act of 1987 established a federal government computer-security program that would protect sensitive information in federal government computer systems and would develop standards and guidelines for unclassified federal computer systems to facilitate such protection. Specifically, the Computer Security Act assigned responsibility for developing government-wide, computer-system security standards and guidelines and security-training programs to the National Bureau of Standards (now the National Institute of Standards and Technology, or NIST). The act also established a Computer System Security and Privacy Advisory Board within the Commerce Department. 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.

In *Information Security and Privacy in Network Environments*, OTA found that implementation of the Computer Security Act has been problematic (see chapter 4 of the 1994 report). In workshop discussions and interviews during and after the assessment, OTA found strong sentiment that agencies follow the rules set forth by the act regarding security plans and training, but do not necessarily fulfill the *intent* of the act. For example, agencies are required to develop security plans—and do—but may not "do the plan" or update plans and implementation in a timely fashion to reflect changes in technology or operations (see section on implementation issues below).

[1] 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).

Implementation of the Computer Security Act has been especially controversial regarding the roles of NIST and National Security Agency (NSA) in standards development for unclassified federal computer systems. The act was designed to balance national security and other national objectives, giving what is now the National Institute of Standards and Technology the lead in developing security standards and guidelines and defining the role of NSA as technical advisor to NIST.[2] However, events subsequent to the act have not convincingly demonstrated NIST's leadership in this area. In OTA's view, NSA has enjoyed de facto leadership in the development of cryptographic standards and technical guidelines for unclassified information security, and implementation of the act has not fulfilled congressional intent in this respect.[3]

EVOLUTION OF POLICY FRAMEWORK FOR UNCLASSIFIED INFORMATION SECURITY[4]

Statutory guidance on safeguarding information provides a policy framework—in terms of technical and institutional requirements and managerial responsibilities—for government information and information-system security. Overlaid on this are statutory privacy requirements that set forth policies concerning the dissemination and use of certain types of information about individuals. Within this framework, and subject to their own specific statutory requirements, federal agencies and departments develop their policies and guidelines, in order to meet individual and government-wide security and privacy objectives.

The **Privacy Act of 1974** (Public Law 93-579) set forth data collection, confidentiality, procedural, and accountability requirements federal agencies must meet to prevent unlawful invasions of personal privacy, and provides remedies for noncompliance. It does not mandate use of specific technological measures to accomplish these requirements. Other statutes set forth information confidentiality and integrity requirements for specific agencies, such as the Internal Revenue Service, Bureau of the Census, and so forth. (Issues related to the Privacy Act, and other, international privacy issues are discussed in chapter 3 of the 1994 OTA report.)

The **Brooks Act of 1965** (Public Law 89-306) was enacted to "provide for the economic and efficient purchase, lease, maintenance, operation, and utilization of automatic data processing [ADP] equipment by federal departments and agencies." *[OTA note: New procurement legislation in the 104th Congress may supersede the Brooks Act.]* The Warner Amendment (Public Law 97-86) subsequently exempted certain types of Defense Department procurements from the Brooks Act (and from section 111 of the Federal Property and Administrative Services Act of 1949).

Among other provisions, the Brooks Act made the Commerce Department the focal point for promulgation of government "automatic data processing" (i.e., computer and information-system) standards and authorized Commerce to conduct a research program to support standards development and assist federal agencies in implementing these standards. These responsibilities were car-

---

[2] NIST recommends standards and guidelines to the Secretary of Commerce for promulgation. Such standards and guidelines would apply to federal computer systems, except for: 1) those systems excluded by section 2315 of Title 10, USC or section 3502(2) of Title 44, USC; and 2) those systems protected at all times by procedures established for information classified by statute or executive order (Public Law 100-235, section 3). The first, "Warner Amendment," exclusion pertains, for example, to intelligence or national security cryptologic systems, mission-critical military or intelligence systems, or systems involving the direct command and control of military forces.

[3] See OTA, op. cit., footnote 1, pp. 138-148, 182-184. See also U.S. General Accounting Office, *Communications Privacy: Federal Policy and Actions,* GAO/OSI-94-2 (Washington, DC: U.S. Government Printing Office, November 1993).

[4] This is taken from OTA, op. cit., footnote 1, ch. 4, esp. pp. 132-138.

ried out by the National Bureau of Standards (now NIST).

NBS established its program in computer and communications security in 1973, under authority of the Brooks Act; the agency was already developing performance standards for government computers. This security program led to the adoption of the Data Encryption Standard (DES) as a federal information processing standard (FIPS) for use in safeguarding unclassified information. The security responsibilities of what is now NIST's Computer Systems Laboratory (CSL) were affirmed and extended by the Computer Security Act of 1987.

The **Paperwork Reduction Act of 1980** (Public Law 96-511) gave agencies a broad mandate to perform their information-management activities in an efficient, effective, and economical manner. [*OTA note: The Paperwork Reduction Act of 1995 was reported on April 3, 1995, and was cleared for the White House on April 6, 1995. The 1995 legislation is discussed in chapter 4 of this background paper. The historical discussion below refers to the 1980 law.*]

The Paperwork Reduction Act of 1980 assigned the Office of Management and Budget (OMB) responsibilities for maintaining a comprehensive set of information resources management policies and for promoting the use of information technology to improve the use and dissemination of information by federal agencies. OMB was given authority for the following: developing and implementing uniform and consistent information resource management policies; overseeing the development of and promoting the use of government information management principles, standards, and guidelines; evaluating the adequacy and efficiency of agency information management practices; and determining whether these practices comply with the policies, principles, standards, and guidelines promulgated by the director of OMB.

OMB Circular A-130 ("Management of Federal Information Resources") was originally issued in 1985 to fulfill these and other statutory requirements (including the Privacy Act). Circular A-130 revised and consolidated policies and procedures from several other OMB directives, which were rescinded. OMB Circular A-130 has recently been revised. The first stage of revisions (June 1993) focused on information exchanges with the public; the second stage addressed agency management practices for information technology and information systems (July 1994). The third stage, addressing security controls and responsibilities in Appendix III of the circular, is ongoing at this writing.

[OTA note: The historical overview of policy development below refers to the 1985 version of Appendix III. OMB's 1995 proposed revision of Appendix III is discussed in chapter 4 of this background paper.]

Appendix III of OMB Circular A-130 (1985) addressed the "Security of Federal Automated Information Systems." Its purpose was to establish a minimal set of controls to be included in federal information systems security programs, assign responsibilities for the security of agency information systems, and clarify the relationship between these agency controls and security programs and the requirements of OMB Circular A-123 ("Internal Control Systems"). The 1985 appendix also incorporated responsibilities from applicable national security directives.

Section 4(a) of the 1985 version of the security appendix of OMB Circular A-130 assigned the Commerce Department responsibility for:

1. developing and issuing standards and guidelines for assuring the security of federal information systems;
2. establishing standards "approved in accordance with applicable national security directives," for systems used to process "sensitive" information, "the loss of which could adversely affect the national security interest;" and
3. providing technical support to agencies in implementing Commerce Department standards and guidelines.

According to the 1985 Appendix III, the Defense Department was to act as the executive agent of the government for the security of telecommunications and information systems that process information, "the loss of which could adversely

affect the national security interest" (i.e., including information that was unclassified but was considered "sensitive"), and was to provide technical material and assistance to federal agencies concerning the security of telecommunications and information systems.

These responsibilities later shifted (see below) in accordance with the Computer Security Act of 1987 and the subsequent National Security Directive 42 (NSD 42). After the Computer Security Act was enacted, NSD 42 set the leadership responsibilities of the Commerce and Defense Departments according to whether the information domain was outside or within the area of "national security."[5]

The **Computer Security Act of 1987** (Public Law 100-235) affirmed and expanded the computer-security research and standards responsibilities of NBS (now NIST) and gave it the responsibility for developing computer system security training programs and for commenting on agency computer system security plans. The Computer Security Act is particularly important because it is fundamental to the development of federal standards for safeguarding unclassified information, to the balance between national security and other objectives in implementing security and privacy policies within the federal government, and to issues concerning government control of cryptography. Moreover, review of the controversies and debate surrounding the Computer Security Act—and subsequent controversies over its implementation—provides background for understanding current issues.

THE COMPUTER SECURITY ACT[6]

The Computer Security Act of 1987 (Public Law 100-235)[7] 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. As noted above, the act established a federal government computer-security program that would protect sensitive information in federal government computer systems and would develop standards and guidelines for unclassified federal computer systems to facilitate such protection.[8] 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. The act also established a Computer System Security and Privacy Advisory Board within the Commerce De-

---

[5] The Computer Security Act of 1987 gave the Commerce Department responsibility in information domains that contained information that was "sensitive" but not classified for national security purposes. National Security Directive 42 *(National Policy for the Security of National Security* [emphasis added] *Telecommunications and Information Systems,* July 5, 1990) established a National Security Telecommunications and Information Systems Security Committee (NSTISSC), made the Secretary of Defense the Executive Agent of the Government for National Security Telecommunications and Information Systems, and designated the Director of NSA as the National Manager for National Security Telecommunications and Information Systems. *[OTA note: This information-security structure may be superseded by a new structure under the Security Policy Board, wherein NSTISSC's functions would be incorporated into the functions of a new Information Systems Security Committee. See chapter 4 and box 1-3 of this paper for discussion of the Security Policy Board.]*

[6] This is taken from OTA, op. cit., footnote 1, ch. 4. See pp. 140-142 of that report for legislative history of the Computer Security Act.

[7] 101 Stat. 1724.

[8] The act was "[t]o provide for a computer standards program within the National Bureau of Standards, to provide for government-wide computer security, and to provide for the training in security matters of persons who are involved in the management, operation, and use of federal computer systems, and for other purposes" (ibid.). Specifically, the Computer Security Act assigned responsibility for developing government-wide, computer-system security standards and guidelines and security-training programs to the National Bureau of Standards (now the National Institute of Standards and Technology). NBS (now NIST) would recommend these to the Secretary of Commerce for promulgation.

partment. (The Computer Security Act and a controversial 1989 Memorandum of Understanding (MOU) laying out the working relationship between NIST and NSA to implement the act are contained in appendix B of the 1994 OTA report).

Congressional concerns and public awareness created a climate conducive to passage of the Computer Security Act of 1987. Highly publicized incidents of unauthorized users, or "hackers," gaining access to computer systems and a growing realization of the government's dependence on information technologies renewed national interest in computer security in the early 1980s.[9]

Disputes over how to control unclassified information also prompted passage of the act. The Reagan Administration had sought to give the National Security Agency much control over what was termed "sensitive, but unclassified" information, while the public—especially the academic, banking, and business communities—viewed NSA as an inappropriate agency for such responsibility. The Reagan Administration favored an expanded concept of national security.[10] This expanded concept was embodied in subsequent presidential policy directives (see below), which in turn expanded NSA's control over computer security. Questions regarding the role of NSA in security for unclassified information, the types of information requiring protection, and the general amount of security needed, all divided the Reagan Administration and the scientific community in the 1980s.[11]

Agency Responsibilities Before the Act

Some level of federal computer-security responsibility rests with the Office of Management and Budget, the General Services Administration (GSA), and the Commerce Department (specifically NIST and the National Telecommunications and Information Administration (NTIA)). OMB maintains overall responsibility for computer security policy.[12] GSA issues regulations for physical security of computer facilities and oversees technological and fiscal specifications for security hardware and software.[13] In addition to its other responsibilities, NSA traditionally has been responsible for security of information that is classified for national security purposes, including Defense Department information.[14] Under the Brooks Act, Commerce develops the federal information processing standards that provide specific codes, languages, procedures, and techniques for use by federal information systems managers.[15] NTIA serves as the executive branch developer of federal telecommunications policy.[16]

These overlapping agency responsibilities hindered the development of one uniform federal policy regarding the security of unclassified information, particularly because computer security

---

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

[10] See, e.g., Harold Relyea, *Silencing Science: National Security Controls and Scientific Communication* (Norwood, NJ: Ablex, 1994).

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

[12] U.S. Congress, House of Representatives, Committee on Science, Space, and Technology, *Computer Security Act of 1987—Report to Accompany H.R. 145,* H. Rept. 100-153, Part I, 100th Cong., 1st sess., June 11, 1987 (Washington, DC: U.S. Government Printing Office, 1987), p. 7.

[13] Ibid.

[14] Ibid.

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

[16] Ibid.

and communications security historically have developed separately. In 1978, OMB had issued Transmittal Memorandum No. 1 (TM-1) to its Circular A-71, which addressed the management of federal information technology.[17] TM-1 required federal agencies to implement computer security programs, but a 1982 General Accounting Office (GAO) report concluded that Circular A-71 (and its TM-1) had failed to provide clear guidance.[18]

Executive orders in the 1980s, specifically the September 1984 National Security Decision Directive 145, "National Policy on Telecommunications and Automated Information Systems Security" (NSDD-145),[19] created significant shifts and overlaps in agency responsibilities. Resolving these was an important objective of the Computer Security Act. NSDD-145 addressed safeguards for federal systems that process or communicate unclassified, but "sensitive" information. NSDD-145 established a Systems Security Steering Group to oversee the directive and its implementation, and an interagency National Telecommunications and Information Systems Security Committee (NTISSC) to guide implementation under the direction of the steering group.[20]

Expanded NSA Responsibilities Under NSDD-145

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

In 1985, the Office of Management and Budget issued another circular concerning computer security. This OMB Circular A-130, "Management of Federal Information Resources," revised and superseded Circular A-71 (see previous section). OMB Circular A-130 defined security, encouraged agencies to consider information security essential to internal control reviews, and clarified the definition of "sensitive" information to include information "whose improper use or disclosure could adversely affect the ability of an agency to accomplish its mission . . . ."[21]

In 1986, presidential National Security Adviser John Poindexter[22] issued "National Telecommunications and Information Systems Security Policy Directive No. 2" (NTISSP No. 2). NTISSP No. 2 proposed a new definition of "sensitive but unclassified information." It potentially could have restricted access to information that previously had been available to the public. Specifically, "sensitive but unclassified information," within the meaning set forth in the directive, included not only information which, if revealed, could adversely affect national security, but also

---

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

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

[19] NSDD-145 is classified. An unclassified version was used as the basis for this discussion.

[20] This became the National Security Telecommunications and Information Systems Security Committee, or NSTISSC. See footnote 5.

[21] Office of Management and Budget, OMB Circular A-130 (1985). At this writing, the proposed revision of Appendix III of A-130 had just been published. The main section of A-130 was revised and issued in 1993.

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

information that could adversely affect "other federal government interests" if released. Other federal government interests included economic, financial, technological, industrial, agricultural, and law enforcement interests.

Such an inclusive directive sparked enormous, negative public response. As the Deputy Director of NBS stated during 1987 hearings on the Computer Security Act, the NTISSP No. 2 definition of sensitive information was a "totally inclusionary definition. . . [t]here is no data that anyone would spend money on that is not covered by that definition."[23] Opponents of NSDD-145 and NTISSP No. 2 argued that NSA should not have control over federal computer security systems that did not contain classified information.[24] The business community, in particular, expressed concern about NSA's ability and suitability to meet the private sector's needs and hesitated to adopt NSA's cryptographic technology in lieu of the DES. At the time, the DES was up for recertification.[25] In the House Report accompanying H.R. 145, the Committee on Science, Space and Technology noted that:

> NSDD-145 can be interpreted to give the national security community too great a role in setting computer security standards for civil agencies. Although the [Reagan] Administration has indicated its intention to address this issue, the Committee felt it is important to pursue a legislative remedy to establish a civilian authority to develop standards relating to sensitive, but unclassified data.[26]

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

> One reason for the assignment of responsibility to NBS for developing federal computer system security standards and guidelines for sensitive information derives from the committee's concern about the implementation of National Security Decision Directive-145.
>
> . . . While supporting the need for a focal point to deal with the government computer security problem, the Committee is concerned about the perception that the NTISSC favors military and intelligence agencies. It is also concerned about how broadly NTISSC might interpret its authority over "other sensitive national security information." For this reason, H.R. 145 creates a civilian counterpart, within NBS, for setting policy with regard to unclassified information. . . NBS is required to work closely with other agencies and institutions such as NSA, both to avoid duplication and to assure that its standards and guidelines are consistent and compatible with standards and guidelines developed for classified systems; but the final authority for developing the standards and guidelines for sensitive information rests with the NBS.[27]

In its report on H.R. 145, the Committee on Government Operations explicitly noted that the bill was "neutral" with respect to public disclosure of information and was not to be used by agencies to exercise control over privately owned information, public domain information, or information

---

[23] Raymond Kammer, Deputy Director, National Bureau of Standards, testimony, "*Computer Security Act of 1987: Hearings on H.R. 145 Before the Subcommittee on Legislation and National Security of the House Committee on Government Operations*," 100th Cong., 1st Sess., Feb. 26, 1987. See also H. Rept. 100-153, Part I, op. cit., footnote 12, p. 18.

[24] See U.S. Congress, House of Representatives, Committee on Science, Space and Technology, *Computer Security Act of 1987: Hearings on H.R. 145 Before the Subcommittee on Science, Research, and Technology and the Subcommittee on Transportation, Aviation, and Materials of the House Committee on Science, Space, and Technology,* 100th Cong., 1st sess. (Washington, DC: U.S. Government Printing Office, 1987), pp. 146-191.

[25] Despite NSA's desire to replace the DES with a family of tamper proof cryptographic modules using classified algorithms, the DES was reaffirmed in 1988.

[26] H. Rept. 100-153, Part I, op. cit., footnote 12, p. 22.

[27] Ibid., p. 26.

disclosable under the Freedom of Information Act or other laws.[28] Furthermore, the committee noted that H.R. 145 was developed in large part to ensure the delicate balance between "the need to protect national security and the need to pursue the promise that the intellectual genius of America offers us." [29] The committee also noted that:

> Since it is a natural tendency of DOD to restrict access to information through the classification process, it would be almost impossible for the Department to strike an objective balance between the need to safeguard information and the need to maintain the free exchange of information.[30]

Subsequent to the Computer Security Act of 1987, the Defense Department's responsibilities under NSDD-145 were aligned by National Security Directive 42 to cover "national security" telecommunications and information systems.[31] NSD 42 did not rescind programs, such as those begun under NSDD-145, that pertained to national security systems, but these were not construed as applying to systems within the purview of the Computer Security Act of 1987.[32]

NSD 42 established the National Security Telecommunications and Information Systems Security Committee, made the Secretary of Defense the Executive Agent of the Government for National Security Telecommunications and Information Systems, and designated the Director of NSA the National Manager for National Security Telecommunications and Information Systems.[33] As such, the NSA Director was to coordinate with NIST in accordance with the Computer Security Act of 1987.

[*OTA note: The proposal for a new, government-wide centralization of unclassified information security, as presented in the November 1994 Security Policy Board staff report, would place the functions of NSTISSC, along with OMB's functions pursuant to Circular A-130, within a new Information Systems Security Committee chaired by DOD and OMB, with NSA as the secretariat. The staff report noted that this was contrary to the Computer Security Act and suggested the need for a strategy to ensure a "smooth transition" to the new structure, including creating a new definition for "national security related information.[34]" See chapter 4 and box 1-3 of this background paper for discussion of the Board staff proposal, along with discussions of other developments, including OMB's proposed revision of Appendix III of OMB Circular A-130 and the Paperwork Reduction Act of 1995.*]

Agency Information-System Security Responsibilities Under the Act

Under the Computer Security Act of 1987, all federal agencies are required to identify computer systems containing sensitive information, and to develop security plans for identified systems.[35] The act also requires mandatory periodic training in computer security for all federal employees and contractors who manage or use federal computer systems. The Computer Security Act gives final

---

[28] U.S. Congress, House of Representatives, Committee on Government Operations, *Computer Security Act of 1987—Report to Accompany H.R. 145*, H. Rept. 100-153, Part II, 100th Cong., 1st sess., June 11, 1987 (Washington, DC: U.S. Government Printing Office, 1987), p. 30.

[29] Ibid., p. 29.

[30] Ibid., p. 29.

[31] National Security Directive 42, op. cit., footnote 5. The National Security Council released an unclassified, partial text of NSD 42 to the Computer Professionals for Social Responsibility on April 1, 1992, in response to Freedom of Information Act (FOIA) requests made in 1990.

[32] Ibid., section 10. The Warner Amendment (Public Law 97-86) had exempted certain types of Defense Department procurements from the Brooks Act.

[33] NSD 42 (unclassified partial text), op. cit., footnote 31, sections 1-7.

[34] Security Policy Board Staff, "Creating a New Order in U.S. Security Policy," Nov. 21, 1994, pp. 17-18.

[35] Public Law 100-235, section 6.

authority to NIST [then NBS] for developing government-wide standards and guidelines for unclassified, sensitive information, and for developing government-wide training programs.

In carrying out these responsibilities, NIST can draw upon the substantial expertise of NSA and other relevant agencies. Specifically, NIST is authorized to "coordinate closely with other agencies and offices," including NSA, OTA, DOD, the Department of Energy, GAO, and OMB.[36] This coordination is aimed at "assur[ing] maximum use of all existing and planned programs, materials, studies, and reports relating to computer systems security and privacy" and assuring that NIST's computer security standards are "consistent and compatible with standards and procedures developed for the protection of information in federal computer systems which is authorized under criteria established by Executive order or an Act of Congress to be kept secret in the interest of national defense or foreign policy."[37] Additionally, the Computer Security Act authorizes NIST to "draw upon computer system technical security guidelines developed by [NSA] to the extent that [NIST] determines that such guidelines are consistent with the requirements for protecting sensitive information in federal computer systems."[38] The act expected that "[t]he method for promulgating federal computer system security standards and guidelines is the same as for non-security standards and guidelines." [39] The intent of the act was that NSA not have the dominant role and to recognize the potential market impact of federal security standards:

> . . . [I]n carrying out its responsibilities to develop standards and guidelines for protecting sensitive information in federal computer systems and to perform research, NBS [now NIST] is required to draw upon technical security guidelines developed by the NSA to the extent that NBS determines that NSA's guidelines are consistent with the requirements of civil agencies. The purpose of this language is to prevent unnecessary duplication and promote the highest degree of cooperation between these two agencies. NBS will treat NSA technical security guidelines as advisory, however, and, in cases where civil agency needs will best be served by standards that are not consistent with NSA guidelines, NBS may develop standards that best satisfy the agencies' needs.
>
> It is important to note the computer security standards and guidelines developed pursuant to H.R. 145 are intended to protect sensitive information in Federal computer systems. Nevertheless, these standards and guidelines will strongly influence security measures implemented in the private sector. For this reason, NBS should consider the effect of its standards on the ability of U.S. computer system manufacturers to remain competitive in the international marketplace.[40]

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

> While the Committee was considering H.R. 145, proposals were made to modify the bill to give NSA effective control over the computer standards program. The proposals would have charged NSA with the task of developing "technical guidelines," and forced NBS to use these guidelines in issuing standards.
>
> Since work on technical security standards represents virtually all of the research effort being done today, NSA would take over virtually the entire computer standards from the National

---

[36] Ibid., section 3(b)(6).

[37] Ibid.

[38] Ibid.

[39] H. Rept. 100-153, Part I, op. cit., footnote 12, p. 26. According to NIST, security FIPS are issued in the same manner as for nonsecurity FIPS. Although the Escrowed Encryption Standard (EES) has classified references, it had the same promulgation method. (F. Lynn McNulty, Associate Director for Computer Security, NIST, personal communication, Mar. 21, 1995.)

[40] Ibid., p. 27.

> Bureau of Standards. By putting NSA in charge of developing technical security guidelines (software, hardware, communications), NBS would be left with the responsibility for only administrative and physical security measures—which have generally been done years ago. NBS, in effect, would on the surface be given the responsibility for the computer standards program with little to say about most of the program—the technical guidelines developed by NSA.
>
> This would jeopardize the entire Federal standards program. The development of standards requires interaction with many segments of our society, i.e., government agencies, computer and communications industry, international organizations, etc. NBS has performed this kind of activity very well over the last 22 years [since enactment of the Brooks Act of 1965]. NSA, on the other hand, is unfamiliar with it. Further, NSA's products may not be useful to civilian agencies and, in that case, NBS would have no alternative but to issue standards based on these products or issue no standards at all.[41]

The Committee on Government Operations also noted the concerns of industry and the research community regarding the effects of export controls and NSA involvement in private sector activities, including restraint of innovation in cryptography resulting from reduced incentives for the private sector to invest in independent research, development, and production of products incorporating cryptography.[42]

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

> The chief purpose of the Board is to assure that NBS receives qualified input from those likely to be affected by its standards and guidelines, both in government and the private sector. Specifically, the duties of the Board are to identify emerging managerial, technical, administrative and physical safeguard issues relative to computer systems security and privacy and to advise the NBS and the Secretary of Commerce on security and privacy issues pertaining to federal computer systems.[43]

The Chair of the CSSPAB is appointed by the Secretary of Commerce. The Board is required to report its findings relating to computer systems security and privacy to the Secretary of Commerce, the OMB Director, the NSA Director, the House Committee on Government Operations, and the Senate Committee on Governmental Affairs.[44]

Implementation Issues

Implementation of the Computer Security Act has been controversial, particularly with respect to the roles of NIST and NSA in standards development. The two agencies developed a Memorandum of Understanding in 1989 to clarify the working relationship, but this MOU has been controversial as well, because of concerns in Congress and elsewhere that its provisions cede NSA much more authority than the act had granted or envisioned.[45] Chapter 4 of the 1994 OTA report examined these implementation issues in depth. It concluded that clear policy guidance and congressional oversight

---

[41] H. Rept. 100-153, Part II, op. cit., footnote 28, pp. 25-26.

[42] Ibid., pp. 22-25, 30-35. In 1986, NSA had announced a program to develop tamper proof cryptographic modules that qualified communications manufacturers could embed in their products. NSA's development of these embeddable modules was part of NSA's Development Center for Embedded COMSEC Products. (NSA press release for Development Center for Embedded COMSEC Products, Jan. 10, 1986.)

[43] H. Rept. 100-153, Part I, op. cit., footnote 12, pp. 27-28.

[44] Public Law 100-235, section 3.

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

will be needed if NIST/NSA processes and outcomes are to reflect a different balance of national security and other objectives, or more openness, than have been evidenced since 1989.

The Computer Security Act of 1987 requires all federal agencies to identify computer systems containing sensitive information, and to develop security plans for these systems.[46] The act also requires mandatory periodic training in computer security for all federal employees and contractors who manage, use, or operate federal computer systems. In its workshops and discussions with federal employees and knowledgeable outside observers, OTA found that these provisions of the Computer Security Act are viewed as generally adequate as written, but that their implementation can be problematic.[47]

During the course of the assessment and follow-on work, OTA found strong sentiment that agencies follow the rules set forth by the Computer Security Act, but not necessarily the full intent of the act. In practice, there are both insufficient incentives for compliance and insufficient sanctions for noncompliance with the spirit of the act. For example, though agencies do develop the required security plans, the act does not require agencies to review them periodically or update them as technologies or circumstances change. One result of this is that "[s]ecurity of systems tends to atrophy over time unless there is a stimulus to remind agencies of its importance."[48] Another result is that agencies may not treat security as an integral component when new systems are being designed and developed.

Ongoing NIST activities in support of information security and privacy are conducted by NIST's Computer Systems Laboratory. In the 1994 report, OTA noted that NIST's funding for these security functions ($4.5 million in appropriated funds for FY 1995) has chronically been low, given NIST's responsibilities under the Computer Security Act. "Reimbursable" funds received from other agencies (mainly DOD) have been substantial ($2.0 million in FY 1995) compared with appropriated funds for security-related activities. Since FY 1990, they have represented some 30 to 40 percent of the total funding for computer-security activities and staff at CSL. This is a large fraction of what has been a relatively small budget (about $6.5 million total in FY 1995).

Some of the possible measures to improve implementation were mentioned during OTA staff interviews and workshops circa 1993-94 including the following: increasing resources for OMB to coordinate and oversee agency security plans and training; increasing resources for NIST and/or other agencies to advise and review agency security plans and training; setting aside part of agency budgets for information security (to be used for risk assessment, training, development, etc.); and/or rating agencies according to the adequacy and effectiveness of their information-security policies and plans and withholding funds until performance meets predetermined accepted levels.

---

[46] Public Law 100-235, section 6.

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

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

Appendix C: U.S. Export Controls on Cryptography

The United States has two regulatory regimes for exports, depending on whether the item to be exported is military in nature, or is "dual-use," having both civilian and military uses. These regimes are administered by the State Department and the Commerce Department, respectively. Both 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[1] 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 that are under Commerce jurisdiction, no specific approval is required and a "general license" applies (e.g., when the item in question is not military or dual-use and/or is widely available from foreign sources). In other cases, an export license must be applied for from either the State Department or the Commerce Department, depending on the nature of the item. In general, the State Department's licensing requirements are more stringent and broader in scope.[2]

---

[1] Both the Export Administration Act (50 U.S.C. App. 2401-2420) and the Arms Export Control Act (22 U.S.C. 2751-2794) provide authority to control the dissemination to foreign nationals (export) of scientific and technical data related to items requiring export licenses under the regulations implementing these acts. "Scientific and technical data" can include plans, design specifications, or other information that describes how to produce an item. See 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), pp. 150-160.

Other statutory authorities for national security controls on scientific and technical data are found in the Restricted Data or "born classified" provisions of the Atomic Energy Act of 1946 (60 Stat. 755) and the Atomic Energy Act of 1954 (68 Stat. 919, 42 U.S.C. 2011-2296), and in the Invention Secrecy Act of 1951 (35 U.S.C. 181-188), which allows for patent secrecy orders and withholding of patents on national security grounds. NSA has obtained patent secrecy orders on patent applications for cryptographic equipment and algorithms under authority of the Invention Secrecy Act.

[2] For another comparison of the two export-control regimes, see U.S. General Accounting Office, *Export Controls: Issues in Removing Militarily Sensitive Items from the Munitions List*, GAO/NSIAD-93-67 (Washington, DC: U.S. Government Printing Office, March 1993), esp. pp. 10-13.

The material in this appendix is taken from pages 150-160 of the 1994 OTA report, updated where appropriate. Licensing terms differ between the agencies, as do time frames and procedures for licensing review, revocation, and appeal.

STATE DEPARTMENT EXPORT CONTROLS ON CRYPTOGRAPHY

The Arms Export Control Act and International Traffic in Arms Regulations (ITAR),[3] administered by the State Department, control export of items (including hardware, software, and technical data) that are "inherently military in character" and, therefore, placed on the Munitions List.[4] Unless otherwise indicated, items on the Munitions List are controlled to all destinations, meaning that "validated" licenses—requiring case-by-case review—are required for any exports (except to Canada, in some cases). The Munitions List is established by the State Department, in concurrence with the Defense Department; the State Department's Office of Defense Trade Controls administers the ITAR and issues licenses for approved exports. The Defense Department provides technical advice to the State Department when there are questions concerning license applications or commodity jurisdiction (i.e., whether State or Commerce regulations apply—see below).

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

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

Several exceptions apply to item XIII(b)(1) above. These include the following subcategories of cryptographic hardware and software:

a. those used to decrypt copy-protected software, provided that the decryption functions are not user-accessible;
b. those used only in banking or money transactions (e.g., in ATM machines and point-of-sale terminals, or for encrypting interbanking transactions);
c. those that use analog (not digital) techniques for cryptographic processing in certain applications, including facsimile equipment, restricted-audience broadcast equipment, and civil television equipment;
d. those used in personalized smart cards when the cryptography is of a type restricted for use only in applications exempted from Munitions List controls (e.g., in banking applications);

---

[3] 22 C.F.R. 120-130.

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

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

e. those limited to access-control functions (e.g., for ATM machines, point-of-sale terminals, etc.) in order to protect passwords, personal identification numbers, and the like provided that they do not provide for encryption of other files or text;
f. those limited to data authentication (e.g., calculating a message authentication code) but not allowing general file encryption;
g. those limited to receiving radio broadcast, pay television, or other consumer-type restricted audience broadcasts, where digital decryption is limited to the video, audio, or management functions and there are no digital encryption capabilities; and
h. those for software designed or modified to protect against malicious computer damage from viruses, and so forth.[6]

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

In September 1994, the State Department announced an amendment to the regulations implementing section 38 of the Arms Export Control Act.[7] The new rule implements one of the reforms applicable to encryption products that were announced on February 4, 1994, by the State Department.[8] It established a new licensing procedure in the ITAR to permit U.S. encryption manufacturers to make multiple shipments of items covered by Category XIII(b)(1) of the Munitions List (see above) directly to end users in an approved country, without obtaining individual licenses. Previously, only those exports covered by a distribution arrangement could be shipped without an individual license; the new procedure permits direct distribution from manufacturers without foreign distributors. The procedures are similar to existing distribution agreement procedures; exporters submit a proposed arrangement specifying items to be shipped, proposed end users and uses, and destination countries. Upon approval, exporters can ship the specified products directly to the end users in the approved countries, with a single license.[9] Among the other reforms announced in February 1994 but awaiting implementation are special licensing procedures that would permit export of key-escrow encryption products to "most" end users.[10]

COMMERCE DEPARTMENT EXPORT CONTROLS ON CRYPTOGRAPHY

The Export Administration Act (EAA)[11] and Export Administration Regulations (EAR),[12] administered by the Commerce Department, are designed to control exports of "sensitive" or dual-use items, including software and scientific and technical data. Some items on the Commerce Control List (CCL) are controlled for national security purposes, to prevent them from reaching "proscribed" countries (usually in the former So-

---

[6] Munitions List, ibid. See XIII(b) (1) (i)-(ix).

[7] 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.

[8] Martha Harris, Deputy Assistant Secretary for Political-Military Affairs, U.S. Department of State, "Encryption—Export Control Reform," statement, Feb. 4, 1994.

[9] *Federal Register*, op. cit., footnote 7, p. 45621.

[10] Martha Harris, op. cit., footnote 8.

[11] At this writing, the export administration legislation is to be reauthorized.

[12] 22 U.S.C. 2751-2794.

viet bloc); others are controlled for various foreign policy objectives.[13]

The Bureau of Export Administration administers controls on dual-use items. The Bureau of Export Administration's Office of Strategic Trade and Foreign Policy Controls [14] is responsible for making licensing determinations, coordinating with other responsible agencies as necessary, and maintaining the Commerce Control List for cryptographic products.[15]

Cryptography falls under Section II ("Information Security") of the CCL.[16] This category includes information-security "equipment, assemblies and components" that:

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

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

OVERLAP BETWEEN CONTROL REGIMES

The "overlap" between the State Department and Commerce Department export-control regimes is particularly complex for cryptography (note the overlap between the Munitions List items and the CCL items shown above, even with the exceptions). Basically, the Commerce Department licenses only those Section II items that are either excepted from State Department control, are not controlled, or are eligible for licensing under an advisory note, plus anti virus software (see item h in the section on State Department controls above).[17] The cryptographic items exempted from control under advisory note 1 are: personalized smart cards as described in item d above; equipment for fixed data compression or coding techniques, or for use in applications described in item g above; portable, commercial civil cellular phones containing encryption, when accompany-

---

[13] See GAO, op. cit., footnote 2, pp. 10-12.

[14] The functions of the Office of Export Licensing and the Office of Technology and Policy Analysis were merged and shifted after a reorganization of the Bureau of Export Administration in late 1994-early 1995. (Maurice Cook, Bureau of Export Administration, Economic Analysis Division, personal communication, Mar. 17, 1995.)

[15] Joseph Young, Office of Strategic Trade and Foreign Policy Controls, Bureau of Export Administration, personal communication, Mar. 23, 1995.

[16] See Supplement 1 to Part 799.1 of the Export Administration Regulations, sections A (equipment, assemblies and components), B (test, inspection, and production equipment), D (software), and E (technology).

[17] Ibid., p. CCL123 (notes). The advisory notes specify items that can be licensed by Commerce under one or more administrative exceptions.

ing their users; and software as described in item a above.[18] Other items, such as cellular phone systems for which message traffic encryption is not possible or items for civilian use in banking, access control, and authentication as described under items b), e), or f) above, are covered by advisory notes 3 through 5. These advisory notes state that these items are likely to be licensed by Commerce, as administrative exceptions, for export to acceptable end users.[19]

At present, software and hardware for robust, user-controlled encryption remains on the Munitions List under State Department control, unless State grants jurisdiction to Commerce.[20] This has become increasingly controversial, especially for the information technology and software industries. According to the U.S. General Accounting Office's (GAO's) 1993 report:

> NSA performs the technical review that determines, for national security reasons, (1) if a product with encryption capabilities is a munitions item or a Commerce List item and (2) which munitions items with encryption capabilities may be exported. The Department of State examines the NSA determination for consistency with prior NSA determinations and may add export restrictions for foreign policy reasons—e.g., all exports to certain countries may be banned for a time period.
>
> . . . [T]he detailed criteria for these decisions are generally classified. However, vendors exporting these items can learn some of the general criteria through prior export approvals or denials they have received. NSA representatives also advise companies regarding whether products they are planning would likely be munitions items and whether they would be exportable, according to State Department representatives.[21]

At the end of COCOM in 1994, the Clinton Administration liberalized the policy for some exports of computer and telecommunications products to Russia, Eastern Europe, and China. However, controls were maintained on cryptography because:

> The President has determined that vital U.S. national security and law enforcement interests compel maintaining appropriate control of encryption.[22]

In 1992, there had been limited relaxation of export controls for mass-marketed software with encryption capabilities. NSA and the State Department relaxed and streamlined export controls for mass-market software with moderate encryption capabilities, but not including software implementing the Data Encryption Standard (DES) or computer hardware containing encryption algorithms.[23] Also, since July 1992, there has been expedited review of software using one of two algorithms developed by RSA Data Security, Inc. These algorithms, called RC2 and RC4, are said to be significantly stronger than those previously allowed for export, but are limited to a 40-bit key length and are said to be weaker than the "DES-strength" programs that can be marketed in the United States and that are available overseas.

U.S. software producers still face the ITAR restrictions (with the new, expedited-distribution rule noted above) for exports of software with strong encryption.[24] Software or hardware products using the DES for message encryption (as opposed to message authentication) are on the Munitions List and are generally nonexportable to foreign commercial users, except foreign subsidiaries of U.S. firms and some financial institutions

---

[18] Ibid., pp. CCL123-126. Software required for or providing these functions is also excepted.

[19] Ibid., Advisory Notes 1-5.

[20] GAO, op. cit., footnote 2, pp. 24-28.

[21] Ibid., p. 25.

[22] Martha Harris, op. cit., footnote 8.

[23] Ibid.

[24] "Strong" encryption in this context refers to systems on a par with the DES or with the RSA system with a 1,024-bit modulus.

(for use in electronic funds transfers). Products that use the DES and other algorithms for purposes other than message encryption (e.g., for authentication) can be exported on the Commerce Control List, however.[25]

In the 103d Congress, legislation intended to streamline controls and ease restrictions on mass-market computer software, hardware, and technology, including certain encryption software, had been introduced. No export legislation was enacted, however, and the last reported version of the House legislation did not include these provisions.[26] In the 104th Congress, omnibus export administration legislation for 1995 has been introduced in the House (H.R. 361). At this writing, it does not have special provisions for cryptography.

[25] GAO, op. cit., footnote 2, p. 26. For discussion of industry and government views, OTA, op. cit., footnote 1, pp. 154-160.

[26] See U.S. Congress, House of Representatives, *Omnibus Export Administration Act of 1994*, H. Rept. 103-531, 103d Cong., 2d sess., Parts 1 (Committee on Foreign Affairs, May 25, 1994), 2 (Permanent Select Committee on Intelligence, June 16, 1994), 3 (Committee on Ways and Means, June 7, 1994), and 4 (Committee on Armed Services, June 17, 1994) (Washington, DC, U.S. Government Printing Office, 1994); and H.R. 4663, "Omnibus Export Administration Act of 1994," June 28, 1994.

D Appendix D: Summary of Issues and Options from the 1994 OTA Report

Part of the motivation for the OTA report *Information Security and Privacy in Network Environments* was the recognition that 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 and sources of online information and entertainment.[1]

The need for congressional attention to safeguarding information has been reinforced in the months since the report was issued in September 1994. The 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.[2] Government agencies have continued to expand both the scale and scope of their network connectivities. Information technologies and networks are featured even more prominently in plans to make government more efficient, effective, and responsive.[3]

Concerns for the security and privacy of networked information remain. In its 1994 report, OTA found that the fast-changing and competitive marketplace that produced the Internet and a strong networking and software industry in the

---

[1] For example, the number of Internet users has been more than doubling each year; some 30 million people worldwide can exchange messages over the Internet. "Browsing" and "chatting" online at home and in the office is increasingly popular—see, e.g., Molly O'Neill, "The Lure and Addiction of Life On Line," *The New York Times*, Mar. 8, 1995, pp. C1, C6.

[2] 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; and 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.

[3] 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.

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 (OMB) (e.g., in OMB Circular A-130), commitment from top agency management, and oversight by Congress. The 1994 OTA report found that in practice, there have historically been both insufficient incentives for compliance, as well as insufficient sanctions for noncompliance, with the spirit of the Computer Security Act.

During the course of the OTA 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 (FIPS) based on cryptography.

The 1994 report focused on policy issues 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. The following sections present the issues and options from that report.

NATIONAL CRYPTOGRAPHY POLICY[4]

The 1994 OTA report concluded that Congress has vital strategic roles in cryptography policy and, more generally, in safeguarding information and protecting personal privacy in a networked society. Because cryptography has become a technology of broad application, decisions about cryptography policy have increasingly broad effects on society. Federal standards (e.g., the federal information processing standards, or the FIPS) and export controls have substantial significance for the development and use of these technologies.

Congressional Review and Open Processes

In 1993, having recognized the importance of cryptography and the policies that govern the development, dissemination, and use of the technology, Congress asked the National Research Council (NRC) to conduct a major study that would support a broad review of cryptography and

[4] See *Information Security and Privacy in Network Environments*, OTA-TCT-606 (Washington, DC; U.S. Government Printing Office, September 1994), pp. 8-18.

its deployment.[5] An important outcome of this review of national cryptography policy would be the development of more open processes to determine how cryptography will be deployed throughout society. Cryptography deployment includes development of the public-key infrastructures and certification authorities that will support electronic delivery of government services, copyright management, and digital commerce.

The results of the NRC study are expected to be available in 1996. But, given the speed with which the Clinton Administration is acting to deploy escrowed encryption within the government, 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. (See also the policy section below on safeguarding information in federal agencies.) 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 NIST and NSA will be a satisfactory part of this open process, or the extent to which the current arrangements should be reevaluated and revised.

Another important outcome 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.

During the assessment, OTA found that many of the persistent concerns surrounding the Escrowed Encryption Standard, and the Clinton Administration's escrowed-encryption initiative generally, focused 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. The National Research Council study should be valuable in helping Congress to understand the broad range of technical and institutional alternatives available for various types of trusteeships for cryptographic keys, "digital powers of attorney," and the like. However, if implementation of the EES and related technologies continues at the current pace, OTA noted that key-escrow encryption may already be embedded in information systems before Congress can act on the NRC report.

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.

[5] For information about the NRC study, contact Herb Lin at the National Research Council (crypto@nas.edu).

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.[6] At this writing, the Commerce Department 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.[7] The study is scheduled to be delivered to National Security Council (NSC) deputies by July 1, 1995. It is anticipated that there will be both unclassified and classified portions of the study; there may be some public release of the unclassified material.[8]

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.

Congressional Responses to Escrowed-Encryption Initiatives

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

The Escrowed Encryption Standard (Clipper) was issued as a voluntary FIPS; use of the EES by the private sector is also voluntary. The Clinton Administration has stated that it has no plans to make escrowed encryption mandatory, or to ban other forms of encryption. 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 to safeguard—among other things—large volumes of private information about individuals (e.g., taxpayer data and health care 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.

In responding to current escrowed-encryption initiatives like the 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.

---

[6] Vice President Al Gore, letter to Representative Maria Cantwell, July 20, 1994. See OTA, op. cit., footnote 4, pp. 11-13.

[7] Maurice Cook, Bureau of Export Administration, Economic Analysis Division, personal communication, Mar. 7, 1995.

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

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.

SAFEGUARDING INFORMATION IN FEDERAL AGENCIES[9]

Congress has an even more direct role in establishing the policy guidance within which federal agencies safeguard information, and in oversight of agency and OMB measures to implement information security and privacy requirements. The Office of Management and Budget is responsible for developing and implementing government-wide policies for information resource management; for overseeing the development and promoting the use of government information-management principles, standards, and guidelines; and for evaluating the adequacy and efficiency of agency information-management practices. During the assessment, OTA found that information-security managers in federal agencies must compete for resources and support to properly implement needed safeguards. For their efforts to succeed, both OMB and top agency management must fully support investments in cost-effective safeguards. Given the expected increase in interagency sharing of data, interagency coordination of privacy and security policies is also necessary to ensure uniformly adequate protection.

Effectiveness of OMB Guidance

The Paperwork Reduction Act of 1995 was signed by President Clinton on May 22, 1995. Both the House (H.R. 830) and Senate (S. 244) versions of the bill reaffirmed OMB's authorities under the Computer Security Act for safeguarding unclassified information. The conference bill[10] containing these provisions passed in both Houses on April 6, 1995 (see chapter 4 of this background paper for discussion).

Appendix III ("Security of Federal Automated Information Systems") of the 1985 version of OMB Circular A-130 set forth OMB's government-wide policy guidance for information security. *At this writing, a new, proposed revision of Appendix III has just been issued.* 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.

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 presented for comment at the end of March 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

---

[9] See OTA, op. cit., footnote 4, pp. 18-20.

[10] See U.S. Congress, House of Representatives, "Paperwork Reduction Act of 1995—Conference Report to Accompany S.244," H.Rpt. 104-99, Apr. 3, 1995. These provisions are found in 44U.S.C. section 3504.

than its measurement, and revise government-wide security responsibilities to be consistent with the Computer Security Act.[11]

See chapter 4 of this background paper for discussion of the proposed revision to Appendix III. The issues and options presented below are in the context of the 1994 report and the 1985 Appendix III. 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.

Because the revised Appendix III had not been issued by the time *Information Security and Privacy in Network Environments* was completed in 1994, the OTA report was unable to assess the revision's potential for improving information security in federal agencies, for holding agency managers accountable for security, or for ensuring uniform protection in light of data sharing and secondary uses. OTA noted that, after the revised Appendix III of OMB Circular A-130 is 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 (GAO). However, the effects of OMB's revised guidance may not be apparent for some time after the revised Appendix III is issued.

Therefore, a few years may pass before GAO is able to report government-wide findings that would be the basis for determining the need for further revision or legislation. In the interim:

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, such as the Internal Revenue Service, that are developing major new information systems. In the course of its oversight and when considering the direction of any new legislation, OTA noted that:

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

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 (NIST) to support its Computer Security Act responsibilities, as well as NIST's other activities related to safeguarding information and protecting privacy in networks.

Regarding NIST's computer-security budget, 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 NIST's information-security activities. However, in staff discussions and workshops during the course of the assessment, OTA found that individuals from outside and within government repeatedly noted that NIST's security activities were not proactive and that NIST often lagged in providing useful and needed standards (the FIPS) and guidelines. Many individuals from the private sector felt that NIST's limited resources for security activities precluded NIST from doing work that would also be useful to industry. Additional resources, whether from overall increases in NIST's budget or otherwise, could enhance

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

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 with respect to standards and guidelines related to cryptography are a special case, however. Increased funding alone will not be sufficient to ensure NIST's technological leadership or its fulfillment of the "balancing" role as envisioned by the Computer Security Act of 1987. With respect to cryptography, 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 Escrowed Encryption Standard (Clipper) was developed and implemented. Increased funding could enable NIST to become a more equal partner to NSA, at least in deploying (if not developing) cryptographic standards. But, if NIST/NSA processes and outcomes are to reflect a different balance of national security and other public interests, or more openness, than has been evidenced over the past five years, OTA concluded that clear policy guidance and oversight (not just funding) will be needed.

LEGAL ISSUES AND INFORMATION SECURITY

The laws currently governing commercial transactions, data privacy, and intellectual property were largely developed for a time when telegraphs, typewriters, and mimeographs were the commonly used office technologies and business was conducted with paper documents sent by mail. Technologies and business practices have dramatically changed, but the law has been slower to adapt. Computers, electronic networks, and information systems are now used to routinely process, store, and transmit digital data in most commercial fields. OTA found that changes in communication and information technologies were particularly significant in three areas: electronic commerce, privacy and transborder data flow, and digital libraries.

Electronic Commerce

As businesses replace conventional paper documents with standardized computer forms, the need arises to secure the transactions and establish means to authenticate and provide *nonrepudiation services for electronic transactions*, that is, a means to establish authenticity and certify that the transaction was made. Absent a signed paper document on which any nonauthorized changes could be detected, a *digital signature* to prevent, avoid, or minimize the chance that the electronic document has been altered must be developed. In contrast to the courts' treatment of conventional, paper-based transactions and records, little guidance is offered as to whether a particular safeguard technique, procedure, or practice will provide the requisite assurance of enforceability in electronic form. This lack of guidance concerning security and enforceability is reflected in the diversity of security and authentication practices used by those involved in electronic commerce.

Legal standards for electronic commercial transactions and digital signatures have not been fully developed, and these issues have undergone little review in the courts. Therefore, OTA noted that immediate action by Congress might not be warranted.[12] However, OTA noted the need for congressional awareness of these issues:

OPTION: Congress could monitor the issue of legal standards for electronic transactions and digital signatures, so that these are considered in future policy decisions about information security.

Such attention would be especially timely, given the increasing focus of the national and international legal communities and the states on developing legal standards for electronic commerce, as well as guidelines and model legislation for digital signatures.

[12] Note this refers to *legal* standards for contracts, rules of evidence, and so forth, not to specific *technical* standards like the DSS.

For example, the American Bar Association's (ABA) Information Security Committee, Science and Technology Section, is drafting "Global Digital Signature Guidelines and model legislation. The ABA effort includes federal-agency representatives, as well as representatives from the private sector and other governments. 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).[13]

Utah has just enacted digital signature legislation. The Utah Digital Signature Act[14] is intended to provide a reliable means for signing computer-based documents and to provide legal recognition of digital signatures using "strong authentication techniques" based on asymmetric cryptography. To assure a minimum level of reliability in digital signatures, the Utah statute provides for the licensing and regulation of certification authorities by a "Digital Signature Agency" (e.g., the Division of Corporations and Commercial Code of the Utah Department of Commerce). The act, first drafted as a proposed model law, provides that the private key is the property of the subscriber who rightfully holds it (and who has a duty to keep it confidential); thus, tort or criminal actions are possible for theft or misuse. It is technology-independent; that is, it does not mandate use of a specific signature technique, although it envisions use of signatures based on standards similar to or including the ANSI X.9.30 or ITU X.509 standards.[15] (Also see discussion in chapter 4 of this background paper.)

Liability issues are also 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.[16]

Protection of Privacy in Data

Since the 1970s, the United States has concentrated its efforts to protect the privacy of personal data collected and archived by the federal government. Rapid development of networks and information processing by computer now makes it possible for large quantities of personal information to be acquired, exchanged, stored, and matched very quickly. As a result, a market for computer-matched personal data has expanded rapidly, and a private sector information industry has grown around the demand for such data.

OTA found that increased computerization and linkage of information maintained by the federal

---

[13] Information on ABA 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).

[14] Utah Digital Signature Legislative Facilitation Committee, "Utah Digital Signature Legislation," Dec. 21, 1994. The Utah Digital Signature Act act was signed into law on Mar. 10, 1995, as section 46-3-101 et seq., Utah Code Annotated. (Prof. Lee Hollaar, University of Utah, personal communication, Mar. 22, 1995.)

[15] Utah Digital Signature Act, ibid. The model legislation was endorsed by the American Bar Association, Information Security Committee of the Science and Technology Section, EDI/Information Technology Division; Prof. Lee Hollaar, University of Utah; Salt Lake Legal Defenders Assoc.; Statewide Association of Public Attorneys; Utah Attorney General's Office; Utah Dept. of Corrections; Utah Information Technology Commission; Utah Judicial Council; and Utah State Tax Commission.

[16] See Michael Baum, op. cit., footnote 12 for discussion of liability exposure, legal considerations, tort and contract remedies, government consent to be liable, and recommendations and approaches to mitigate liability.

government is arguably not addressed by the Privacy Act, which approaches privacy issues on an agency-by-agency basis. To address these developments, OTA noted several alternatives:

OPTION: Congress could allow each agency to address privacy concerns individually, through its present system of review boards.

OPTION: Congress could require agencies to improve the existing data integrity boards, with a charter to make clearer policy decisions about sharing information and maintaining its integrity.

OPTION: Congress could amend the existing law to include provisions addressing the sharing and matching of data, or restructure the law overall to track the flow of information between institutions.

OPTION: Congress could provide for public access for individuals to information about themselves, and protocols for amendment and correction of personal information. It could also consider providing for online publication of the Federal Register *to improve public notice about information collection and practices.*

OTA noted that, in deciding between courses of actions, Congress could exercise its responsibility for oversight through hearings and/or investigations, gathering information from agency officials involved in privacy issues, as well as citizens, in order to gain a better understanding of what kinds of actions are required to implement better custodianship, a minimum standard of quality for privacy protection, and notice to individuals about use and handling of information.

Although the United States does not comprehensively regulate the creation and use of such data in the private sector, foreign governments (particularly the European Union) do impose controls. The Organization for Economic Cooperation and Development (OECD) adopted guidelines in 1980 to protect the privacy and transborder flows of personal data. The difference between the level of personal privacy protection in the United States and that of its trading partners, who in general more rigorously protect privacy, could inhibit the exchange of data with these countries. U.S. business has some serious concerns about the European Union (EU) proposal, as it relates to the data subject's consent and the transfer of data to non-EU countries. OTA noted that Congress had a choice when addressing the sufficiency of existing U.S. legal standards for privacy and security in a networked environment for the private sector:

OPTION: Congress could legislate to set standards similar to the OECD guidelines;

or,

OPTION: Congress could allow individual interests, such as the business community, to advise the international community on its own of its interests in data protection policy. However, because the EU's protection scheme could affect U.S. trade in services and could impact upon individuals, Congress may also wish to monitor and consider the requirements of foreign data protection rules as they shape U.S. security and privacy policy to assure that all interests are reflected.

OTA noted that a diversity of interests must be reflected in addressing the problem of maintaining privacy in computerized information—whether in the public or private sector. To deal with this, OTA noted that:

OPTION: Congress could establish a Federal Privacy Commission.

Proposals for such a commission or board were previously discussed by OTA in its 1986 report *Electronic Record Systems and Individual Privacy.* In that study, OTA cited the lack of a federal forum in which the conflicting values at stake in the development of federal electronic systems could be fully debated and resolved. As privacy questions will arise in the domestic arena, as well as internationally, a commission could deal with these as well.

Protection of Intellectual Property in the Administration of Digital Libraries

OTA found that the availability of protected intellectual property in *digital libraries* and other networked information collections is straining the traditional methods of protection and payment for use of intellectual property. Technologies (like digital signatures and encryption) developed for safeguarding information might also hold promise for monitoring the use of copyrighted informa-

tion and facilitating means for collecting royalties and compensating the copyright holders. The application of intellectual-property law to protect works maintained in digital libraries continues to be problematic; traditional copyright concepts such as *fair use* are not clearly defined as they apply to these works; and the means to monitor compliance with copyright law and to distribute royalties is not yet resolved.

OTA had addressed these legal and institutional issues in an earlier report, *Finding a Balance: Computer Software, Intellectual Property, and the Challenge of Technological Change*. The 1992 report included several options to deal with the use of works in electronic form.

During the 1994 assessment, OTA found that the widespread development of multimedia authoring tools—integrating film clips, images, music, sound, and other content—raises additional issues pertaining to copyright and royalties. With respect to copyright for multimedia works, OTA noted that:

OPTION: Congress could allow the courts to continue to define the law of copyright as it is applied in the world of electronic information;

or,

OPTION: Congress could take specific legislative action to clarify and further define the copyright law in the world of electronic information.

Instead of waiting for legal precedents to be established or developing new legislation, OTA noted that Congress might try a third approach that would allow producer and user communities to establish common guidelines for use of copyrighted, multimedia works:

OPTION: Congress could allow information providers and purchasers to enter into agreements that would establish community guidelines without having the force of law. In so doing, Congress could decide at some point in the future to review the success of such an approach.

More generally, with respect to private sector solutions for problems concerning rights and royalties for copyrighted works in electronic form, OTA noted that:

OPTION: Congress could encourage private efforts to form rights-clearing and royalty-collection agencies for groups of copyright owners.

Alternatively,

OPTION: Congress might allow private sector development of network tracking and monitoring capabilities to support a fee-for-use basis for copyrighted works in electronic form.

In the latter case, Congress might wish to review whether a fee-for-use basis for copyrighted works in electronic form is workable, from the standpoint of both copyright law and technological capabilities. OTA suggested that this might be accomplished by conducting oversight hearings, undertaking a staff analysis, and/or requesting a study from the Copyright Office.

Index

A

Accredited Standards Committee X9, 20, 82
Advanced Research Projects Agency, 19, 81
Algorithms. *See* Cryptographic algorithms
American Bar Association
  Science and Technology Section's Information Security Committee, 23, 87, 129
Arms Export Control Act, 12-13, 63, 117
ARPA. *See* Advanced Research Projects Agency
ASC X9. *See* Accredited Standards Committee X9
Association for Computing Machinery
  EES policy issues report, 21, 85
  U.S. Public Policy Committee of the ACM, 21-22, 85
Asymmetric cryptosystems. *See* Public-key cryptography
ATM machines, 117, 118
AT&T Corp.
  encryption microchip development, 20, 56, 82
AT&T CryptoBackup, 83
AT&T Surity Telephone Device, 20, 82
Authentication
  cryptography and, 47, 48
  definition, 6
Authenticity
  definition, 3

B

Background paper
  description, 2
  overview of chapters, 3-42
  purpose, 23
Bankers Trust International Corporate Key Escrow, 21, 83
Banking and financial services industries
  cryptography and, 20, 82, 117-118
Bell Atlantic Key Escrow, 83
"Best practices" of businesses, 68-71
Bill of Rights for privacy, 71
Branstad, Dennis, 82-83
Brickell, Ernest, 55
Brooks Act of 1965, 106-107
Bureau of Export Administration, 119
"Business Requirements for Encryption," 22, 86
Businesses. *See* Private sector; *specific businesses by name*

C

Canada
  privacy policy, 71
Cantwell, Rep. Maria, 13, 63
Capstone chip
  costs, 18, 35, 80, 98
  escrow locations, 17
  lack of market support for, 20, 82
  use by Defense Message System, 79
Cellular phones, 119-120
China
  liberalization of exports to, 120
Ciphertext
  description, 46, 48
Cleartext
  description, 46
Clinton Administration. *See also* Escrowed-encryption initiative; Escrowed Encryption Standard; Executive branch
  centralization of information security authorities, 8, 27, 53
  commitment to escrowing encryption keys, 17-18, 79
  creation of interagency working group on encryption and telecommunications, 56
  easing of export controls on cryptography without legislation, 14, 64
  exportability of EES encryption products, 54
  international market studies, 63
  liberalization of export controls, 120
  market study of cryptography and export controls, 97-98
  NIST funding, 81
  plans for making escrowed encryption mandatory, 37, 53, 125

Clipper chip. *See* Escrowed Encryption Standard
COCOMM. *See* Coordinating Committee for Multilateral Export Controls
Code of Fair Information Practices, 24, 89
Collins, Rep. Cardiss, 23, 88
Commerce Department. *See* Department of Commerce
Committee on Government Operations
  report on H.R. 145, 111-112
Competitiveness
  U.S. export policy and, 67
Computer crime, 72
Computer Security Act of 1987, 53
  agency responsibilities, 42, 109-110, 112-114
  controversies over, 910, 60, 92, 105-106, 114-115
  cost-effective safeguards, 41, 101
  description, 9, 60
  evolution of policy framework, 106-108
  frustration over implementation of, 74
  fulfilling intent of the act, 105, 115
  hearings on, 111
  implementation issues, 9-10, 15-16, 39, 42, 105, 114-115
  incentives for compliance and sanctions for noncompliance, 123
  mandates, 78
  NIST responsibilities, 9-10, 42, 113-114, 127-128
  NSA responsibilities, 9-10, 110-112, 113-114
  OMB Circular A-130 Appendix III proposed revision and, 29, 32, 126
  overlapping agency responsibilities before, 109-110
  oversight of, 16, 42, 68, 74, 98
  provisions, 10, 91, 105, 108-115
Computer System Security and Privacy Advisory Board, 10, 27, 60, 74, 105, 108-109, 114
  Resolution 95-3, 92
Computer Systems Laboratory, 107, 115
Computer Systems Policy Project
  GII recommendations, 21, 84-85
Confidentiality
  definition, 3
Congress. *See also* Government; Legislation; *specific committees, pieces of legislation, and members of Congress by name*
  cryptography policy review, 34-35, 123-124
  escrowed encryption initiatives responses, 36-37, 42, 125-126
  export administration legislation, 13, 63, 64, 121
  export controls and, 13, 14, 35-36, 63, 68, 73, 97-98, 121
  federal information security and privacy oversight, 37-38, 40-41, 98
  implications for action, 34-42, 97-101
  issues and options, 4, 34-42, 122-131
  letter of request to OTA, 2, 104
  locus of authority for information security, 39-42, 100-101
  OMB Circular A-130 Appendix III proposed revision oversight, 39, 40
  privacy protection legislation, 88-89
  workshop views on areas of action needed, 73-75
Cooperative research and development agreements
  for Westinghouse Savannah River Company to develop DSS software, 80
Coordinating Committee for Multilateral Export Controls, 120
Copyrighted materials
  digital signatures and, 47
  fee-for-use, 131
  options for protecting, 130-131
  workshop views, 71-72
Corporate privacy, 72, 75
Crackers, 2
CRADAs. *See* Cooperative research and development agreements
"Creating a New Order in U.S. Security Policy," 26-27, 91-92, 94
Credit reports, 24, 88
Crime
  computer crime, 72
  cryptography control and, 7
  organized crime, 78
Cryptanalysis
  description, 47
Cryptographic algorithms. *See also specific algorithms by name*
  description, 46
"Cryptographic Service Calls," 19, 81
Cryptography
  applications of, 56
  background, 5
  congressional review and open processes, 34-35, 123-124
  description, 3, 45, 46
  executive branch developments, 79-81
  history of, 46
  importance of, 57, 45-50
  misuse potential, 52
  nongovernmental markets, 6, 50
  policy debate over, 50, 52-53
  private sector developments, 82-84
  terminology, 46-47
  uses for, 46-47
Cryptography control
  Computer Security Act of 1987 and, 60
  as domestic security issue, 52-53
  export controls, 6, 7-8, 11-14, 35-36, 52-53, 61-64, 66-68, 116-121, 123, 124-125
  government marketplace influence, 60-61

issues and options, 4, 64
lack of dialogue between government and private sector on, 15, 67-68, 73-74, 101
leadership and responsibility issues, 78, 15, 53, 68
mechanisms, 7, 50
as national security issue, 50, 52
policy objectives, 7
tension between promoting and controlling information safeguards, 50
Cryptosystems. *See also specific system by name*
description, 46-47
CSL. *See* Computer Systems Laboratory
CSPP. *See* Computer Systems Policy Project
CSSPAB. *See* Computer System Security and Privacy Advisory Board

D

Damages
for misuse or unauthorized disclosure of escrowed key components, 37, 126
Data Encryption Standard
EES algorithm comparison, 54
export policy and, 67
key length, 57
reaffirmation of, 57
as stable technology, 11, 61
successors, 9, 57
triple DES version, 9, 56, 57
"Data Encryption Standard" (FIPS Publication 46-2), 57
Databases
key escrowing or trusteeship for, 18, 79
national identification database, 23, 88
Decrypting, 117
Decryption keys, 6
Defense Information Systems Agency, 19, 81
mock attacks, 78
Defense Message System, 9, 53, 80
Denning, Dorothy, 55, 82-83
Department of Commerce. *See also* Computer System Security and Privacy Advisory Board
Commerce Control List, 118-119
deposit of encryption keys in, 79
economic impact of U.S. export controls on U.S. software industry, 13, 36, 125
EES proposal, 8, 54
export controls, 11-12, 13, 62, 63, 116, 118-121
OMB Circular A-130 Appendix III proposed revision guidance, 33, 96
responsibilities before Computer Security Act of 1987, 109
traditional responsibilities for security standards, 100
Department of Defense, 53. *See also* Defense Information Systems Agency
Defense Message System, 9, 53, 80
export controls, 117
Information Warfare activities, 24-25, 78, 89
mock attacks on computers, 78
OMB Circular A-130 Appendix III proposed revision guidance, 33, 96
Department of Energy
UNIX flaw alert, 77
Department of Justice
EES proposal, 54
OMB Circular A-130 Appendix III proposed revision guidance, 33, 96
Department of State
Arms Export Control Act amendment, 12-13, 63
export controls, 11-13, 62, 82, 116-118, 119-121
model law on electronic data interchange, 23, 87, 129
Office of Defense Trade Controls, 117
Department of the Treasury
deposit of encryption keys in, 79
EES escrow agent, 55
DES. *See* Data Encryption Standard
Diffie-Hellman key exchange, 21, 58, 59
Digital libraries, 130-131
Digital Signature Act, 87-88, 129
Digital Signature Standard
costs, 8081
description, 49
government-wide implementation, 80
patent problems, 18, 79-80
public-key algorithm specified in, 9, 57
RSA and, 18, 20, 49, 80
Digital signatures
acceptance and use of new FIPS for, 18
alternatives to, 49
description, 3, 6, 48-49
electronic commerce and, 4, 128-129
message authentication and, 47, 48
public-key cryptography and, 47
Utah statute, 87-88
DISA. *See* Defense Information Systems Agency
DOD. *See* Department of Defense
"Draft Principles for Providing and Using Personal Information and Commentary," 24, 89
Drug testing
as privacy issue, 88
DSS. *See* Digital Signature Standard

E

Eastern Europe. *See also* Europe
liberalization of exports to, 120
Economic espionage, 78

EES. *See* Escrowed Encryption Standard
Electronic commerce
  digital signatures and, 4, 128-129
  nonrepudiation services, 128
Electronic Record Systems and Individual Privacy, 130
Employees
  Computer Security Act of 1987 training requirements, 112-113, 115
  errors due to lack of training in security, 70
Encryption
  definition, 3, 56
Escrowed encryption
  description, 45
Escrowed-encryption initiative, 6, 45
  congressional responses to, 36-37, 42, 125-126
  controversy over, 4, 123
  costs, 35, 98
Escrowed Encryption Standard. *See also* Skipjack algorithm
  ACM report, 85
  alternatives to, 17, 79
  Clinton Administration policy, 35, 53
  closed process for developing and implementing, 15, 41, 128
  DES algorithm comparison, 54
  description, 67, 89, 53, 54
  functions, 54-55
  history of, 55-56
  lack of market support for, 20, 82
  as mandatory, 8, 37, 124, 125
  private sector acceptance, 15, 61
  "spare keys" for, 7
  uses, 9, 45
  voluntary use of by private sector, 125
Europe. *See also* Eastern Europe
  need for consistency between U.S. privacy laws and European privacy laws, 75
  privacy policies, 71
European Union, 130
Exclusionary Rule Reform Act of 1995, 23-24, 88
Executive branch
  alternatives to EES and Skipjack, 79
  cryptography developments, 79-81
  digital signatures, 79-81
  reaction to ISSC, 27, 92
Executive Order 12333, 110
Executive orders
  agency responsibilities and, 110
Export Administration Act
  reauthorization, 36, 97-98
Export Administration Act of 1995, 14, 64
Export Administration Regulations, 118
Export controls
  Arms Export Control Act amendment, 12-13, 63
  on cryptography, 6, 7-8, 11-14, 35-36, 52-53, 61-64, 66-68, 116-121, 123, 124-125
  liberalization of, 120
  licensing requirements, 11-12, 62, 63, 116-121
  military and dual-use items, 11, 61-62, 116
  omnibus export administration legislation, 63, 121
  proliferation of cryptography to foreign adversaries and, 12, 62-63
  workshop views on congressional action needed, 14-15, 66-68, 73, 97

F

"Fair use" concept, 131
Family Privacy Bill, 24, 88-89
Federal Bureau of Investigation, 73
Federal information processing standards. *See also specific standards and titles by name*
  DES and, 8, 9
  DSS and, 8, 9
  EES promulgated as, 8-9, 45
  escrowed-encryption initiative and, 4
  for secure key exchange, 79
  Skipjack and, 8-9, 79
  users' needs and, 98
Federal Manager's Financial Accountability Act, 97
Federal Register
  online publication of, 130
Financial services. *See* Banking and financial services industry
Finding a Balance: Computer Software, Intellectual Property, and the Challenge of Technological Change, 131
FIPSs. *See* Federal information processing standards
Firewalls, 78
FORTEZZA PCMCIA cards
  costs, 18-19, 80-81, 98
  Defense Message System use, 79
  nondefense agency adoption of, 35
  number in use, 53, 56
Fortress KISS, 83

G

General Accounting Office
  export controls, 120
  OMB Transmittal Memorandum No. 1 and, 110
  study request, 127
General Services Administration
  government public-key infrastructure, 81
  OMB Circular A-130 Appendix III proposed revision guidance, 33, 96
  responsibilities before Computer Security Act of 1987, 109
GII. *See* Global information infrastructure

Glenn, Sen. John
letter of request, 2, 104
"Global Digital Signature Guidelines," 23, 87
Global information infrastructure, 21, 84-86
Gore, Albert. *See also* Vice President's National Performance Review
encryption market and export controls study, 36, 125
letter to Representative Cantwell, 13, 63
Government. *See also* Clinton Administration; Congress; Executive branch; Executive orders; Private sector; Reagan Administration; *specific agencies by name*
agency downsizing and restructuring effects on information security, 98-99
cryptography control efforts, 4, 6, 7-8, 50, 52-53, 56-64
dialogue between government and private sector, 15, 67-68, 73-74, 97-98
export controls, 6, 52-53, 61-64, 97-98
federal agency head responsibilities under Paperwork Reduction Act of 1995, 95
information security in federal agencies, 74-75, 98-101
information security regarded as "expensive overhead" by agency managers, 98-99
key-escrow encryption alternatives, 83-84
locus of authority for information security, 39-42, 100-101
management commitment to security, 4, 17, 38, 74, 94, 97, 98-99, 123
marketplace influence attempts, 60-61, 69
OMB Circular A-130 Appendix III proposed revisions, 95-97, 99-100
proposals for centralizing security responsibilities, 8, 100-101
safeguarding information in federal agencies, 126-128
safeguarding unclassified information, 98-101
tension between promoting and controlling information safeguards, 50
Government Information Technology Services Public-Key Infrastructure Federal Steering Committee, 19, 81

H

Hackers, 109
Hashing algorithms, 49
Hashing functions, 48-49
Horn, Rep. Steve, 24, 88
House Committee on Foreign Affairs, 13, 63
House Permanent Select Committee on Intelligence, 13, 63
House Subcommittee on Telecommunications and Finance, 2

I

ICC. *See* International Chamber of Commerce
"ICC Position Paper on International Encryption Policy," 22, 85-86
IEEE P1363
working group on public-key cryptography, 20-21, 82
Immigration concerns, 23, 88
Individual Privacy Protection Act of 1995, 23, 88
Information infrastructure
global information infrastructure, 21, 71, 84-86
Information Infrastructure Task Force
Working Group on Privacy, 24, 89
Information security
definition, 3
"Information Security and Privacy in Network Environments: What Next?." *See* Workshop
Information-security policy initiatives and legislation
Joint Security Commission, 25-90, 100-101
locus of authority for, 39-42, 100-101
OMB Circular A-130 Appendix III proposed revision, 29, 32-34, 95-97
Paperwork Reduction Act of 1995, 28-29, 94-95
Security Policy Board, 25-28, 90-94
Information Systems Security Committee, 26-27, 39, 91-92, 100
Information Systems Security Research Joint Technology Office, 19-20, 24, 81, 89
Integrity of information
cryptography and, 46-47
definition, 3, 6
Intellectual property. *See also* Copyrighted materials
options for protecting, 4, 130-131
workshop views, 71-73
"Internal Control Systems," 107
International Chamber of Commerce
cryptography position paper, 22, 85-86
model law on electronic data interchange, 23, 87, 129
International issues. *See also* Export controls; *specific countries and regions by name*
cryptography markets, 6
DES-based encryption and authentication methods use, 20, 82
personal data transfer, 130
privacy policies, 71
USCIB recommendations, 86
International Traffic in Arms Regulations, 117, 118
Internet, 122

lack of built-in security, 69
unauthorized intrusions, 2
ISSC. *See* Information Systems Security Committee
ITAR. *See* International Traffic in Arms Regulations

J
Joint Security Commission
efficiency arguments, 100-101
information security recommendations, 89-90
JTO. *See* Information Systems Security Research Joint Technology Office

K
Katzen, Sally
letter from Steering Committee of the Federal Computer Security Program Manager's Forum, 27, 92-93
Privacy Protection Commission statement, 88
Kent, Stephen, 55
Key-escrow encryption. *See also* Escrowed encryption; Public-key cryptography
alternatives to, 17, 21, 82-84
damages for misuse or unauthorized disclosure of escrowed key components, 37, 126
export controls and, 52-53
market appeal, 11
rationale for, 6
Key management, 47
Keys
commercial depositories, 79
decryption keys, 6
deposit in Commerce and Treasury departments, 79
description, 46-47
EES "spare keys," 7
key escrowing or trusteeship for large databases, 18, 79
optional deposit with registries, 17-18, 79
size and encryption scheme strength, 47

L
Lab document confidentiality, 72
Law enforcement, 52
Law Enforcement Access Field, 54, 55
LEAF. *See* Law Enforcement Access Field
Legal issues
confidentiality of corporate information, 72
copyrighted materials, 4, 47, 71-72, 130-131
digital signatures, 23, 87
electronic commerce, 128-129
intellectual property protection, 130-131
personal privacy protection, 129-130
Legislation. *See also* Congress; *specific pieces of legislation by name*
privacy protection, 23-24, 88-89
Letter of request from Roth and Glenn, 2, 104
Liability issues
business uncertainty about U.S. government's position on, 86-87
importance to electronic commerce development, 22-23, 87
personal data and, 72-73, 129-130
"Liability Issues and the U.S. Administration's Encryption Initiatives," 22, 86
Licensing requirements. *See* Export controls
Locus of authority for information security, 39-42, 100-101

M
Maher, David, 55
Mailing lists
sale of by communication carriers or U.S. Postal Service, 24, 88
Management
federal agency security responsibilities, 4, 17, 38, 74, 94, 97, 98-99, 123
private sector security responsibilities, 4, 16, 17, 68, 70-71, 123
"Management of Federal Information Resources," 107, 110
Marketing. *See also* Export controls
government efforts to control, 11, 60-61, 69
security problems in, 69
technology stability and, 10-11, 61
Medical privacy rights, 88
Memorandum of Agreement establishing JTO, 81
Memorandum of Understanding between NIST and NSA, 74, 109, 114
Message authentication
definition, 3
digital signatures and, 47, 48
Micali Fair Cryptosystems, 83
MOU. *See* Memorandum of Understanding between NIST and NSA
Multimedia works
copyright for, 131
Munitions List, 63, 117, 118, 119, 120
Murray, Sen. Patty, 13, 63
Mykotronx, 20, 54, 82

N
National Bureau of Standards. *See* National Institute of Standards and Technology
National identification database, 23, 88
National Institute of Standards and Technology, 73
DSS product validation system, 19, 81

EES escrow agent, 55
funding, 15-16, 19, 41, 42, 74-75, 81, 115, 127-128
Memorandum of Understanding with NSA, 74, 109, 114
redirection of activities, 39, 68, 98
responsibilities under Computer Security Act of 1987, 9-10, 42, 60, 105, 106, 112-113
"National Policy on Telecommunications and Automated Information Systems Security," 110
National Research Council
cryptography study, 13-14, 35, 64, 123-124
National Security Agency
absolute effectiveness standard versus cost-effectiveness, 41, 101
assessment of economic impact of U.S. export controls on U.S. software industry, 13, 36, 125
expanded responsibilities under NSDD-145, 110-112
foreign availability of encryption products study, 63-64
frustration over role of, 73-74
JTO establishment, 19
Memorandum of Understanding with NIST, 74, 109, 114
responsibilities under Computer Security Act of 1987, 9-10, 106, 113-114
Skipjack development, 8
Trusted Computer System Evaluation Criteria, 117, 119
National Security Council, 13, 54, 125
National Security Decision Directive 145, 92, 110-112
National Security Directive 42, 108
National Telecommunications and Information Administration, 109
National Telecommunications and Information Systems Security Committee, 110
"National Telecommunications and Information Systems Security Policy Directive No. 2," 110-111
NBS. *See* National Institute of Standards and Technology
Network information
decentralization, 5, 44
focus on safeguarding the information itself, 5, 44, 97
1994 OTA report
background, 44-45
cryptography importance, 45-50
current report and, 2
government efforts to control cryptography, 50, 52-53, 56-64
issues and options, 64, 122-131
motivation for, 122
need for products that integrate security features with other functions, 123
overview, 43-64
preparation request, 2
summary, 4
workshop participants and, 65
NIST. *See* National Institute of Standards and Technology
Nonrepudiation services for electronic transactions, 128
NSA. *See* National Security Agency
NSD 42. *See* National Security Directive 42
NSDD-145. *See* National Security Decision Directive 145
NTIA. *See* National Telecommunications and Information Administration
NTISSP No. 2. *See* "National Telecommunications and Information Systems Security Policy Directive No. 2"

O

OECD. *See* Organization for Economic Cooperation and Development
Office of Management and Budget, 53, 88. *See also specific OMB circulars by number*
effectiveness of guidance, 126-128
notice of "Draft Principles for Providing and using Personal Information and Commentary," 24, 89
Paperwork Reduction Act responsibilities, 94-95
responsibilities before Computer Security Act of 1987, 109
security policy guidance, 4, 123
Office of Personnel Management
OMB Circular A-130 Appendix III proposed revision guidance, 33, 96
Office of Strategic Trade and Foreign Policy Controls, 119
OMB. *See* Office of Management and Budget
OMB Circular A-71
Transmittal Memorandum No. 1, 110
OMB Circular A-123, 107
OMB Circular A-130, 107, 110
OMB Circular A-130 Appendix III, 107-108
OMB Circular A-130 Appendix III proposed revision, 78, 93
active risk acceptance and accountability by management, 33, 97
cost-effective safeguards, 41-42, 101
free information flow and public accessibility and, 27
guidance provisions, 29, 32, 33-34, 38-39, 40, 95-96

intention, 95, 126-127
shift in emphasis to safeguarding information itself, 5, 97
Omnibus Export Administration Act of 1994, 13, 63
Open Systems Interconnection protocols for networking, 60
Open User Recommended Solutions, 69-70
Organization for Economic Cooperation and Development, 130
Organized crime, 78
OSI protocols. *See* Open Systems Interconnection protocols for networking
OURS. *See* Open User Recommended Solutions

P

Paperwork Reduction Act of 1980, 107
Paperwork Reduction Act of 1995, 92
agency responsibilities, 28-29, 78
cost-effective safeguards, 29, 41, 101
provisions, 28-29, 94-95, 97
reaffirmation of OMB responsibilities, 29, 126
Passwords
employees' posting of passwords on computers, 70
password sniffers, 2, 77
Patents, 18, 72
Digital Signature Standard and, 79-80
PCMCIA cards. *See* FORTEZZA PCMCIA cards
PDD-29. *See* Presidential Decision Directive 29
Personal Computer Memory Card Industry Association cards. *See* FORTEZZA PCMCIA cards
Personal data
liability standards, 72-73, 75, 129-130
potential for abuse of information, 71
"Perspectives on the Global Information Infrastructure," 21
PKI. *See* Public-Key Infrastructure Federal Steering Committee
Plaintext
description, 46, 48
Poindexter, John, 110-111
Point of sale terminals, 117, 118
Presidential Decision Directive 29
items it was not intended to cover, 26, 91
Security Policy Board and Security Policy Advisory Board creation, 25, 26, 90-91
Privacy
definition, 3
medical privacy rights, 88
need for consistency between U.S. laws and European laws, 75
privacy protection legislation, 23-24, 88-89
workshop view, 71
Privacy Act
OMB Circular A-130 Appendix III proposed revision and, 29, 126
Privacy Act of 1974
provisions, 106
Privacy Bill of Rights, 71
Privacy Commission, 71, 75, 130
Privacy Protection Commission, 23, 88
Private sector. *See also* Government; *specific businesses by name*
availability of secure products, 69-70
common checklist for security officers, 70-71
cost concerns, 15, 69-70
cryptography developments, 20-21, 82-84
dialogue between government and, 15, 67-68, 73-74, 97-98
domestic and international privacy issues, 14-15, 71
global information infrastructure, 21, 84-86
information-security policies and "best practices," 68-71
large business and small business ability to purchase product incorporating security, 69
management responsibility for information security, 4, 16, 17, 68, 70-71, 123
preference for RSA over DSS, 80
technology-neutral security policies, 16, 68-69, 99
training issues, 70
voluntary use of EES, 11, 125
Proprietary information
workshop views, 71-73
Public-key cryptography. *See also* Digital Signature Standard
description, 6, 46-47, 48, 51
digital signatures and, 47, 48-49
secret-key distribution using, 58
Public-Key Infrastructure Federal Steering Committee, 81

R

RC2 algorithm, 20, 120
RC4 algorithm, 120
RC5 algorithm, 82
Reagan Administration
role of NSA, 109
Reno, Janet, 55
Rivest-Shamir-Adleman algorithm
description, 9, 48
DSS and, 18, 49, 80, 82
export policy and, 67
for secure key exchange, 58
signature creation, 49
Roth, Rep. Toby, 14, 64

Roth, Sen. William V., Jr.
letter of request, 2, 104
Royalties, 130-131
RSA algorithm. *See* Rivest-Shamir-Adleman algorithm
RSA Data Security, Inc.
RC5 algorithm, 20, 82
RC2 and RC4 algorithms, 120
Russia
liberalization of exports to, 120

S

Safeguard
definition, 3
Search and seizure issues, 23, 88
Secret-key cryptography
description, 46-47, 48, 50
"Security of Federal Automated Information." *See* OMB Circular A-130 Appendix III proposed revision
Security Policy Advisory Board, 26, 90-91
Security Policy Board
creation, 25, 90
Information Systems Security Committee, 25-27, 39, 91-92, 100
membership, 25, 90
OMB Circular A-130 Appendix III proposed revision guidance, 33, 96
opposition to recommendations, 92-93
Security Policy Forum, 90
staff comments on OTA draft text, 28, 94
staff report, 8, 26-27, 30-32, 91-92, 94, 100
"Security Policy Coordination," 25
Security Policy Forum, 25-26, 90
"Security Requirements for Cryptographic Modules" (FIPS 140-1), 19, 81
Senate Committee on Governmental Affairs, 2
Senate Committee on the Judiciary
Title V of S.3 hearing, 24, 88
Signature digitalization. *See* Digital signatures
Simon, Sen. Paul, 88
Single-key systems. *See* Secret-key cryptography
Skipjack algorithm
alternatives to, 17, 79
as DES successor, 57
description, 89, 54, 56-57
evaluation by outside experts, 55
key length, 56
uses, 8, 9, 18, 53
Smart cards, 117, 119
Sniffers, 2, 77
Social security cards
tamper proofing, 23, 88
Software
Commerce Department and NSA assessment of economic impact of U.S. export controls on U.S. software industry, 13, 36, 125
copyright for multimedia works, 131
export controls, 12, 62, 63, 118, 120
ITAR restrictions, 120-121
Software Publishers Association, 62*n*
SPB. *See* Security Policy Board
Spoofing, 77
State Department. *See* Department of State
Steering Committee of the Federal Computer Security Program Manager's Forum
letter to Sally Katzen, 27, 92-93
Subscriber list sale, 24, 88
Symmetric encryption. *See* Secret-key cryptography
Systems Security Steering Group, 110

T

TCP/IP protocols. *See* Transmission Control Protocol/Internet Protocol
Technology-neutral information-security policies, 16, 68-69, 99
TECSEC VEIL, 83
Terminology, 4
Terrorism, 7, 52, 78
TESSERA cards. *See* FORTEZZA PCMCIA cards
TIS. *See* Trusted Information Systems, Inc.
TIS Commercial Software Key Escrow System, 83
TIS Software Key Escrow System, 83
Training
Computer Security Act of 1987 requirements, 112-113, 115
employee errors and security systems, 70
materials for, 70
private sector problems, 17, 70
Transmission Control Protocol/Internet Protocol, 60-61
Trusted Computer System Evaluation Criteria, 117, 119
Trusted Information Systems, Inc.
key-escrow encryption alternative, 21, 83-84
key-escrow system description, 56
Tuchman, Walter, 55

U

United Nations Commission on International Trade Law
model law on electronic data interchange, 23, 87, 129
United States Council for International Business
position papers, 22-23, 86-87
UNIX operating system, 69
DOE's alert to flaw in, 77

U.S. Postal Service
government public-key infrastructure, 81
sale of mailing lists, 24, 88
U.S. Public Policy Committee of the ACM
recommendations, 21-22, 85
USACM. *See* U.S. Public Policy Committee of the ACM
USCIB. *See* United States Council for International Business
Utah
Digital Signature Act, 87-88, 129

V

Vice President's National Performance Review, 88
VLSI Logic, 54
VLSI Technology, Inc.
encryption microchip development, 20, 56, 82

W

Warner Amendment, 10, 60, 106
Westinghouse Savannah River Company, 80
Workshop
discussion topics, 14-17, 35-36, 66, 67, 97
objectives, 14, 66
participant demographics, 14, 65-66
private sector information-security policies, 68-75
purpose, 65
World Wide Web
home page flaw, 77
products under development, 77-78