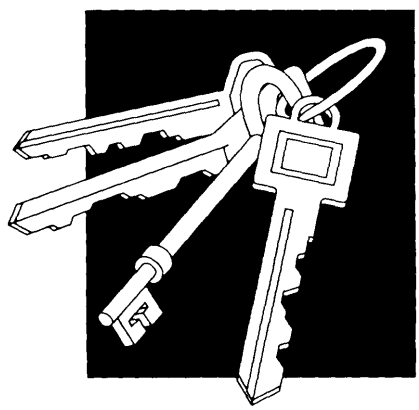
Introduction and Policy Summary 1

The technology used in daily life is changing. Information technologies are transforming the ways we create, gather, process, and share information. Computer networking is driving many of these changes; electronic transactions and records are becoming central to everything from commerce to health care. The explosive growth of the Internet exemplifies this transition to a *networked society.* According to the Internet Society, the number of Internet users has doubled each year; this rapid rate of growth increased more during the first half of 1994. By July 1994, the Internet linked over 3 million host computers worldwide; 2 million of these Internet hosts are in the United States. [1] Including users who connect to the Internet via public and private messaging services, some 20 to 30 million people worldwide can exchange messages over the Internet.

OVERVIEW

The use of information networks for business is expanding enormously. [2] The average number of electronic point-of-sale transactions in the United States went from 38 per day in 1985 to 1.2



[1] Data on Internet size and growth from the Internet Society, press release, Aug. 4, 1994. The Internet originated in the Department of Defense's ARPANET in the early 1970s. By 1982, the TCP/IP protocols developed for ARPANET were a military standard and there were about 100 computers on [he ARPANET. Twelve years later, the Internet links host computers in more than 75 countries via a network of separately administered networks.

[2] See U.S. Congress, Office of Technology Assessment, *Electronic Enterprises: Looking to the Future*, OTA-TCT-600 (Washington, DC U.S. Government Printing Office, May I 99-$).

million per day in 1993.[3] An average $800 billion is transferred among partners in international currency markets every day; about $1 trillion is transferred daily among U.S. banks; and an average $2 trillion worth of securities are traded daily in New York markets.[4] Nearly all of these financial transactions pass over information networks.

Government use of networks features prominently in plans to make government more efficient, effective, and responsive.[5] Securing the financial and other resources necessary to successfully deploy information safeguards can be difficult for agencies, however. Facing pressures to cut costs *and* protect information assets, some federal-agency managers have been reluctant to connect their computer systems and networks with other agencies, let alone with networks outside government.[6] Worse, if agencies were to "rush headlong" onto networks such as the Internet, without careful planning, understanding security concerns, and adequate personnel training, the prospect of plagiarism, fraud, corruption or loss of data, and improper use of networked information could affect the privacy, well-being, and livelihoods of millions of people.[7]

In its agency audits and evaluations, the General Accounting Office (GAO) identified several recent instances of information-security and privacy problems:

- In November 1988, a virus caused thousands of computers on the Internet to shut down. The virus's primary impact was lost processing time on infected computers and lost staff time in putting the computers back on line. Related dollar losses are estimated to be between $100,000 and $10 million. The virus took advantage of UNIX's trusted-host features to propagate among accounts on trusted machines. (U.S. General Accounting Office, *Computer Security: Virus Highlights Need for Improved Internet Management,* GAO/l M-TEC-89-57 (Washington, DC: U.S. Government Printing Office, June 1989).)
- Between April 1990 and May 1991, hackers penetrated computer systems at 34 Department of Defense sites by weaving their way through university, government, and commercial systems on the Internet. The hackers exploited a security hole in the Trivial File Transfer Protocol, which allowed users on the Internet to access a file containing encrypted passwords without logging onto the system. (U.S. General Accounting Office, *Computer Security: Hackers Penetrate DOD Computer Systems,* GAO/ IMTEC-92-5 (Washington, DC: U.S. Government Printing Office, November 1991).)
- Authorized users of the Federal Bureau of Investigation's National Crime Information Center misused the network's information. Such misuse included using the information to, for example, determine whether friends, neighbors, or relatives had criminal records, or inquire about backgrounds for political purposes. (U.S. General Accounting Office, *National*

---

[3] Electronic Funds Transfer Association, Herndon, VA. Based on data supplied by *Bunk Network News* and *POS News*.

[4] Joel Kurtzman, *The Death of Money* (New York, NY: Simon & Schuster, 1993).

[5] See *The National Information Infrastructure: Agenda for Action,* Information Infrastructure Task Force, Sept. 15, 1993; and *Reengineering Through Information Technology,* Accompanying Report of the National Performance Review (Washington, DC: Office of the Vice President, 1994). See also U.S. Congress, Office of Technology Assessment, *Making Government Work: Electronic Delivery of Federal Services,* OTA-TCT-578 (Washington, DC: U.S. Government Printing Office, September 1993).

6 This was one finding from a series Of agency visits made by the Office of Management and Budget (OMB), the National Institute of Standards and Technology (NIST), and the National Security Agency (NSA) in 1991 and 1992. The visits were made as part of the implementation of the Computer Security Act of 1987 and the revision of the security sections of OMB Circular A-130 (see ch. 4). See Office of Management and Budget, "Observations of Agency Computer Security Practices and implementation of OMB Bulletin No. 90-08," February 1993.

[7] See F. Lynn McNuhy, Associate Director for Computer Security, National Institute of Standards and Technology, "Security on the Internet," testimony presented before the Subcommittee on Science, Committee on Science, Space, and Technology, U.S. House of Representatives, Mar. 22, 1994, p. 8.

Crime Information Center: Legislation Needed To Deter Misuse of Criminal Justice Information, GAO/T-GGD-93-41 (Washington, DC: U.S. Government Printing Office, July 1993).)

= In October 1992, the Internal Revenue Service's (IRS's) internal auditors identified 368 employees who had used the IRS's Integrated Data Retrieval System without management knowledge, for non-business purposes. Some of these employees had used the system to issue fraudulent refunds or browse taxpayer accounts that were unrelated to their work, including those of friends, neighbors, relatives, and celebrities. (U.S. General Accounting Office, *IRS Information Systems: Weaknesses Increase Risk of Fraud and Impair Reliability of Management Information, GAO/AIMD-93-34* (Washington, DC: U.S. Government Printing Office, September 1993).)[8]

More recent events have continued to spur government and private-sector interest in information security:

- A series of *hacker attacks* on military computers connected to the Internet has prompted the Defense Information Systems Agency to tighten security policies and procedures in the defense information infrastructure. The hackers, operating within the United States and abroad, have reportedly penetrated hundreds of sensitive, but unclassified, military and government computer systems. The break-ins have increased significantly since February 1994, when the Computer Emergency Response Team first warned that unknown intruders were gathering Internet passwords by using what are called *sniffer programs. The* sniffer programs operate surreptitiously, capturing authorized users' logins and passwords for later use by intruders. The number of captured passwords in this series of attacks has been estimated at a million or more, potentially threatening all the host computers on the Internet--and their users.[9]

The Networked Society

The transformation being brought about by networking brings with it new concerns for the security and privacy of networked information. If these concerns are not properly resolved, they threaten to limit networking's full potential, in terms of both participation and usefulness. Thus, *information safeguards* are achieving new prominence.[10] Whether for use in government or the private sector, appropriate information safeguards, must account for—and anticipate—technical, institutional, and social developments that increasingly shift responsibility for safeguarding information to the end users.

Key developments include the following:

- There has been an overall movement to *distributed computing.* Computing power used to be concentrated in a mainframe with '*dumb" desktop terminals. Mainframes, computer workstations, and personal computers are increasingly connected to other computers through direct connections such as local- or wide-area networks, or through modem connections via telephone lines. Distributed computing is relatively informal and bottom up;

[8]Examples provided by Hazel Edwards, Director, General Government Information Systems, U.S. General Accounting office, personal communication, May 5, 1994.

[9]See Elizabeth Sikorovsky, "Rome Lab Hacker Arrested After Lengthy Invasion," *Federal Computer Week,* July 18, 1994, p. 22; Peter H. Lewis, "Hackers on Internet Posing Security Risks, Experts Say," *The New York Times,* July21, 1994, pp. 1, B 10; Bob Brewin, "DOD To Brief White House on Hacker Attacks," *Federal Computer Week,* July 25, 1994, pp. 1, 4.

[10]In this report 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 its discussion of information safeguards, this report focuses on technical and institutional measures to ensure the *confidentiality* and *integrity* of the information and the *authenticity* of its origin.

systems administration may be less rigorous as it is decentralized.

- *Open systems* allow interoperability among products from different vendors. Open systems shift more of the responsibility for information security from individual vendors to the market as a whole.
- *Boundaries between types of information are blurring.* As the number of interconnected computers and users expands, telephone conversations, video segments, and computer data are merging to become simply digital information, at the disposal of the user.
- The number and variety of *service providers* has increased. A decade after the divestiture of AT&T, the market is now divided among many local-exchange and long-distance carriers, cellular carriers, satellite service providers, value--added carriers, and others. Traditional providers are also entering new businesses: telephone companies are testing video services; some cable television companies are providing telephone and Internet services; Internet providers can deliver facsimile and video information; electric utilities are seeking to enter the communications business.
- *Lower costs* have moved computing from the hands of experts. Diverse users operate personal computers and can also have access to modems, encryption tools, and information stored in remote computers. This can empower individuals who might otherwise be isolated by disabilities, distance, or time. Lower cost computing also means that businesses rely more on electronic information and information transfer, But, lower cost computing also empowers those who might intrude into personal information, or criminals who might seek to profit from exploiting the technology. Potential intruders can operate from anywhere in the world if they can find a vulnerability in the network.
- Computer networks allow more *interactivity.* Online newspapers and magazines allow readers to send back comments and questions to reporters; online discussion groups allow widely dispersed individuals to discuss diverse issues; pay-per-view television allows viewers to select what they want to see. Consequently, providers must consider new responsibilities—such as protecting customer privacy[11]—resulting from interactivity.
- Information technology has done more than make it possible to do things faster or easier—*electronic commerce* has transformed and created industries. Successful companies depend on the ability to identify and contact potential customers; customer buying habits and market trends are increasingly valuable as businesses try to maximize their returns. Manufacturing is becoming increasingly dependent on receiving and making shipments "just in time" and no earlier or later to reduce inventories. Documents critical to business transactions—including electronic funds—are increasingly stored and transferred over computer net works.
- Electronic information has opened new questions about *copyright, ownership, and responsibility for information.* Rights in paper-based and oral information have been developed through centuries of adaptation and legal precedents. Information in electronic form can be created, distributed, and used very differently than its paper-based counterparts, however.
- Measures to *streamline operations* through use of information technology and networks require careful attention to technical and institutional safeguards. For example, combining personal records into a central database, in or-

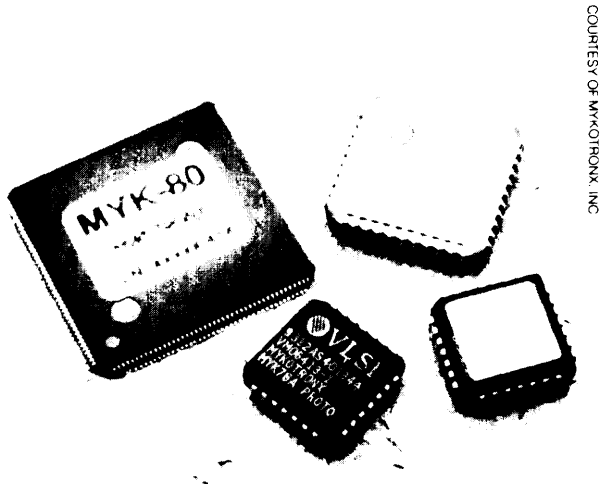
[1] In this report OTA uses the term *confidentiality* to refer to disclosure of information only to authorized individuals, entities, and so forth. *Privacy* refers to the social balance between an individual right to keep information confidential and the societal benefit derived from sharing information, 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.

der to improve data processing efficiency, can put privacy at risk if adequate safeguards are not also implemented. In addition, many types of information safeguards are still relatively new, and methods to balance risks and the costs of protecting information are not fully developed.

Distributed computing and open systems can make every user essentially an "insider." This means that responsibility for safeguarding information becomes distributed as well, potentially putting the system at greater risk. With the rapid changes in the industry, the responsibilities of each network provider to other providers and to customers may not be as clear as in the past. Even though each player may be highly trusted, the overall level of trust in the network necessarily decreases, unless the accountability of each of the many intermediaries is very strict. Thus, users must take responsibility for safeguarding information, rather than relying on intermediaries to provide adequate protection.

Background of the OTA Assessment

In May 1993, Senator William V. Roth, Jr., Ranking Minority Member of the Senate Committee on Governmental Affairs, requested that the Office of Technology Assessment (OTA) study the changing needs for protecting (unclassified) information and for protecting the privacy of individuals, given the increased connectivity of information systems within and outside government and the growth in federal support for large-scale networks. Senator Roth requested that OTA assess the need for new or updated federal computer-security guidelines and federal computer-security and encryption standards. Senator John Glenn, Chairman of the Senate Committee on Governmental Affairs, joined in the request, noting that it is incumbent for Congress to be informed and ready to develop any needed legislative solutions for these emerging information-security and privacy issues. Congressman Edward J. Markey, Chairman of the House Subcommittee on Telecommunications and Finance, also joined in endorsing the study (see request letters in appendix A). After consultation with requesting staff, OTA prepared a proposal for an expedited study; the proposal was approved by the Technology Assessment Board in June 1993.



COURTESY OF MYKOTRONX, INC.

The Clipper chip.

This report focuses on safeguarding unclassified *information* in networks, not on the security or survivability of networks themselves, or on the reliability of network services to ensure information access. The report also does not focus on "computer crime" per se (a forthcoming OTA study, *Information Technologies for Control of Money Laundering,* focuses on financial crimes). This study was done at the unclassified level. Project staff did not receive or use any classified information during the course of the study.

The widespread attention to and the significance of the Clinton Administration's escrowed-encryption initiative resulted in an increased focus on the processes that the government uses to regulate *cryptography* and to develop *federal information processing standards* (the FIPS) based on cryptography. Cryptography is a fundamental technology for protecting the confidentiality of information, as well as for checking its integrity and authenticating its origin.

Cryptography was originally used to protect the confidentiality of communications, through

encryption; it is now also used to protect the confidentiality of information stored in electronic form and to protect the integrity and authenticity of both transmitted and stored information. With the advent of what are called *public-key* techniques, cryptography came into use for *digital signatures* that are of widespread interest as a means for electronically authenticating and signing commercial transactions like purchase orders, tax returns, and funds transfers, as well as for ensuring that unauthorized changes or errors are detected. These functions are critical for electronic commerce. Techniques based on cryptography can also help manage copyrighted material and ensure its proper use.

This study builds on the previous OTA study of computer and communications security, *Defending Secrets, Sharing Data: New, Locks and Keys for Electronic Information,* OTA-CIT-310 (Washington, DC: U.S. Government Printing Office, October 1987). The 1987 study focused on security for unclassified information within relatively closed networks. Since then, new information security and privacy issues have resulted from advances in networking, such as the widespread use of the Internet and development of the information infrastructure, and from the prospect of networking as a critical component of private and public-sector functions. These advances require appropriate institutional and technological safeguards for handling a broad range of personal, copyrighted, sensitive, and proprietary information. This study also builds on intellectual-property work in *Finding a Balance: Computer Software, Intellectual Property, and the Challenge of Technological Change, OTA-TCT-527* (Washington, DC: U.S. Government Printing Office, May 1992); the analysis of issues related to digital libraries and other networked information resources in *Accessibility and Integrity of Networked Information Collections,* BP-TCT-109 (Washington, DC: OTA, August 1993); and the analysis of privacy issues in *Protecting Privacy in Computerized Medical Information,* OTA-TCT-576 (Washington, DC: U.S. Government Printing Office, September 1993).

In addition to meetings and interviews with experts and stakeholders in government, the private sector, and academia, OTA broadened participation through the study's advisory panel and through four project workshops (see list of workshop participants in appendix D). The advisory panel met in April 1994 to discuss a draft of the report and advise the project staff on revisions and additions. To gather expertise and perspectives from throughout OTA, a "shadow panel" of 11 OTA colleagues met with project staff as needed to discuss the scope and subject matter of the report.

At several points during the study, OTA staff met formally and informally with officials and staff of the National Institute of Standards and Technology (NIST) and the National Security Agency (NSA). Individuals from these agencies, as well as from the Office of Management and Budget (OMB), the Office of Science and Technology Policy, the Department of Justice, the Federal Bureau of Investigation, the General Services Administration, the Patent and Trademark Office, the Copyright Office, the General Accounting Office, and several mission agencies, were among the workshop participants and were invited to review a draft of the report (see list of reviewers who provided comments in appendix E).

SAFEGUARDING NETWORKED INFORMATION

The information infrastructure is already international: networks like the Internet seamlessly cross national borders. Networked information is similarly borderless. Achieving consensus regarding information safeguards among the diverse stakeholders worldwide is more difficult than solving many technical problems that might arise. The federal government can help resolve many of these interrelated issues. But they must be solved systematically, not piecemeal, in order to attain an overall solution.

This report focuses on policy issues and options regarding cryptography policy, guidance on safeguarding information in federal agencies, and

legal issues of electronic commerce, personal privacy, and copyright. These policy issues and options are summarized in the next section of this chapter. The remainder of this section summarizes other findings regarding the development and deployment of safeguard technologies (for a detailed discussion, see chapter 2).

The fast-changing and competitive marketplace that produced the Internet and a strong networking and software industry in the United States has not consistently produced products equipped with affordable, easily used safeguards. In general, many individual products and techniques are currently available to adequately safeguard specific information networks—provided the user knows what to purchase, and can afford and correctly use the product. Nevertheless, better and more affordable products are needed. In particular, there is a need for products that *integrate* security features with other functions for use in electronic commerce, electronic mail, or other applications.

More study is needed to fully understand vendors' responsibilities with respect to software and hardware product quality and liability. More study is also needed to understand 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 products. Broader efforts to safeguard networked information will be frustrated unless cryptography-policy issues are resolved (see chapter 4).

A *public-key infrastructure* (PKI) is a critical underpinning for electronic commerce and transactions. The establishment of a system of certification authorities and legal standards, in turn, is essential to the development of a public-key infrastructure and to safeguarding business and personal transactions. Current PKI proposals need further development and review, however, before they can be deployed successfully.

Ideally, the safeguards an organization implements to protect networked information should reflect the organization's overall objectives. In practice, this is often not the case. Network designers must continuously struggle to balance utility, cost, and security. Information can never be absolutely secured, so safeguarding information is not so much an issue of how to secure information as one of how much security a government agency or business can *justify.*

There is a great need for federal agencies, as well as other organizations, to develop more robust *security policies* that match the reality of modem information networks. These policies should support the specific agency objectives and interests, including but not limited to policies regarding private information. The policies must also anticipate a future where more information may be shared among agencies. Finally, these policies should be mandated from the highest level.

The single most important step toward implementing proper safeguards for networked information in a federal agency or other organization is for its 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.

Both *risk analysis* and *principles of due care* need further development. Neither approach is necessarily always appropriate and therefore neither is always sufficient to provide a strong defense against liability in the case of a monetary loss related to loss, theft, or exposure of networked information. A combination of the two approaches will likely provide improved protection. Before *formal models* can be successful for safeguarding the exchange of information among government agencies or other organizations, the entities must first review and coordinate their information-security policies. These policies can then be implemented according to new or existing formal models as needed. OTA found in its interviews, however, that while exploration into new types of formal models maybe warranted, there is considerable doubt about the utility of formal models for safeguarding networked information,

particularly to protect the integrity and availability of information.

The federal government *trusted product evaluation process* is not, and will not soon be, effective for delivering products that adequately protect unclassified information in network environments. Alternatives to that approach appear promising, however, including (but not limited to) NIST's Trusted Technology Assessment Program. *Generally Accepted System Security Principles* (GSSP) also have strategic importance for establishing *due care* guidelines for cost-justifying safeguards, as targets for training and professional programs, and as targets for insurance coverage. The current federal effort in GSSP will not produce immediate results, but the effort is overdue and OTA found wide support for its mission. Efforts to "professionalize" the information security field are important, but will not produce significant results for some time. Success depends significantly upon the success of Generally Accepted System Security Principles and their adoption in industry and government.

Emergency response efforts are vital to safeguarding networked information, due to the relative lack of shared information about vulnerabilities on information networks. Expanding current efforts could further improve the coordination of system administrators and managers charged with protecting networked information.

Criminal and civil sanctions constitute only one aspect of safeguarding networked information. Further study is needed to determine the effectiveness of such sanctions, as opposed to improving the effectiveness of law enforcement to act on existing laws. With the rapid expansion of the networked society, there is a great need to support reevaluation of *fundamental ethical principles*-—work that is currently receiving too little attention. More resources also could be applied to study and improve the methods and materials used in education of ethical use of networked information, so that more effective packages are available to schools and organizations that train users. Finally, more resources could also be directly applied to educate users (including federal employees, students, and the public at large) about ethical behavior.

POLICY ISSUES AND OPTIONS

This report focuses on policy issues in three 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. Chapter 4 discusses cryptography policy and guidance on safeguarding information in federal agencies. It examines the current public controversies regarding the Clinton Administration's escrowed-encryption initiative and the development of new federal information processing standards based on cryptography. Because the Computer Security Act of 1987 (Public Law 100-235) is significant for both development of the FIPS and agency guidance on safeguarding information, chapter 4 also examines the act in some depth, including the continuing controversies concerning its implementation and the working relationship between NIST and NSA.

Chapter 3 examines legal issues including: discussion of nonrepudiation services and digital signatures for electronic commerce; the Privacy Act of 1974 and the implications for the United States of privacy initiatives in the European Union; and copyright for networked information and multimedia works.

National Cryptography Policy

The federal government faces a fundamental tension between two important policy objectives: 1) fostering the development and widespread use of cost-effective information safeguards, and 2) controlling the proliferation of safeguard technologies that can impair U.S. signals-intelligence and law-enforcement capabilities. This tension runs throughout the government activities as a developer, user, and regulator of safeguard technologies. This tension is manifested in concerns over the proliferation of cryptography that could im-

pair U.S. signals intelligence and law enforcement, and in the resulting struggle to control cryptography through use of federal standards and export controls.

Despite the growth in nongovernmental cryptographic research and safeguard development over the past 20 years, the federal government still has the most expertise in cryptography.[12] Therefore, the federal information processing standards developed by NIST substantially influence the development and use of safeguards based on cryptography in the private sector as well as in government.[13] The nongovernmental market for cryptography-based products has grown in the last 20 years or so, but is still developing, Export controls also have substantial significance for the development and use of these technologies. Therefore, Congress's choices in setting national cryptography policies (including standards and export controls) affect information security and privacy in society as a whole.

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

Policy debate over cryptography used to be as arcane as the technology itself. Most people didn't regard government decisions about cryptography as directly affecting their lives. However, as the communications technologies used in daily life have changed, concern over the implications of privacy and security policies dominated by national security objectives has grown dramatically y, particularly in business and academic communities that produce or use information safeguards, but among the general public as well. This concern is reflected in the ongoing debates over *key-escrow encryption* and the government's Escrowed Encryption Standard (EES).[14]

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. 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. More widespread foreign use of cryptography—including use by terrorists and developing countries-makes U.S. signals intelligence more difficult. Within the United States, cryptography is increasingly 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

---

12 The governmental monopoly on cryptography has been eroding. Over the past three decades, the government's struggle for control has been exacerbated by technological advances m computing and microelectronics that have made inexpensive cryptography potentially ubiquitous, and by increasing private-sector capabilities m cryptography (as evidenced by independent development of commercial, public-key encryption systems). These developments have made possible the Increasing reliance on digital communications and information processing for commercial transactions and operations in the public and private sectors. Together, they have enabled and supported a growing industry segment offering a variety of hardware- and software-based in formation safeguards based on cryptography.

13 With respect to information safeguards based on cryptography, national-security concerns shape the safeguard standards (i.e., the FIPS) available to agencies for safeguarding unclassified in formation. Therefore, these concerns also affect civilian agencies that are usual]) not thought of in conjunction with national security.

14 The EES is intended for use in safeguarding voice, facsimile, or computer data communicated in a telephone system. The Clipper chip is designed for use in telephone systems; it contains the EES encryption algorithm, called SKIPJACK. The Clipper chip is being used in the AT&T Surity Telephone Device 3600, which has a retail price of about $1,100.

recognition of the potential misuses of cryptography, 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 intended to preserve U.S. law-enforcement and signals-intelligence capabilities.

Federal Information Processing Standards Based on Cryptography

The Escrowed Encryption Standard has been promulgated by the Clinton Administration as a voluntary alternative to the original federal encryption standard used to safeguard unclassified information, the Data Encryption Standard (DES). A *key-escrowing* scheme is built in to ensure lawfully authorized electronic surveillance when key-escrow encryption is used (see box 2-7 and box 4-2). The federal Digital Signature Standard (DSS) uses a public-key signature technique but does not offer public-key encryption or key-management functions (see box 4-4). Therefore, it cannot support secure exchange of cryptographic keys for use with the DES or other encryption algorithms.

In OTA's view, both the EES and the DSS are federal standards that are part of a long-term control strategy intended to retard the general availability of "unbreakable" or "hard to break" cryptography within the United States, for reasons of national security and law enforcement. It appears that the EES is intended to complement the DSS in this overall encryption-control strategy, by discouraging future development and use of encryption without built-in law enforcement access, in favor of key-escrow encryption and related technologies. Wide use of the EES and related technologies could ultimately reduce the variety of other cryptography products through market dominance that makes the other products more scarce or more costly.

Concerns over the proliferation of encryption that have shaped and/or retarded federal standards development have complicated federal agencies' technological choices. For example, as appendix C explains, national security concerns regarding the increasingly widespread availability of robust encryption-and, more recently, patent problems-contributed to the extraordinarily lengthy development of a federal standard for digital signatures: NIST first published a solicitation for public-key cryptographic algorithms in 1982, and the DSS was finally approved in May 1994.

Public-key cryptography can be used for digital signatures, for encryption, and for secure distribution or exchange of cryptographic keys. The DSS is intended to supplant, at least in part, the demand for other public-key cryptography by providing a method for generating and verifying digital signatures. However, while the DSS algorithm is a public-key *signature* algorithm, it is not a public-key *encryption* algorithm (see box 4-4). That means, for example, that it cannot be used to securely distribute "secret" encryption keys, such as those used with the DES algorithm (see figure 2-4). Some sort of interoperable (i.e., standardized) method for secure key exchange is still needed. [15] As this report was completed, the DSS had been

[15] One public-key algorithm that can be used for key distribution is the "RSA" algorithm; the RSA algorithm can encrypt. The RSA system was proposed in 1978 by Ronald Rivest, Adi Shamir, and Leonard Adleman. The Diffie-Hellman technique is another method for key generation and exchange; it does not encrypt (see figure 2-5).

issued, but there was no FIPS for public-key key exchange.[16]

The lengthy evolution of the DSS meant that federal agencies had begun to look to commercial products (e.g., based on the Rivest-Shamir-Adleman, or *RSA*, system) to meet immediate needs for digital signature technology. The introduction of the EES additionally complicates agencies' technological choices, in that the EES and related government key-escrowing techniques (e.g., for data communication or file encryption) for may not become popular in the private sector for some time, if at all. As this report was finalized, the EES has not yet been embraced within government and is largely unpopular outside of government. Therefore, agencies may need to support multiple encryption technologies both for transactions (i.e., signatures) and for communications (i.e., encryption, key exchange) with each other, with the public, and with the private sector.

In July 1994, Vice President Al Gore indicated the Clinton Administration's willingness to explore industry alternatives for key-escrow encryption, including techniques based on unclassified algorithms or implemented in software.[17] These alternatives would be used to safeguard information in computer networks and video networks; the EES and Clipper chip would be retained for telephony. Whether the fruits of this exploration result in increased acceptance of key-escrow encryption within the United States and abroad will not be evident for some time.

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 originating in the United States, or to re-export these from another country. Licensing requirements vary according to the nature of the item to be exported, the end use, the end user, and, in some cases, the intended destination. For many items, no specific approval is required and a '*general license" applies (e.g., when the item in question is not military or dual-use and/or is wide] y 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.[18]

Software and hardware for robust, user-controlled encryption are under State Department control. unless State grants jurisdiction to Commerce. This has become increasingly controversial, especial] y for the information technology and software industries. The impact of export controls

---

16 Two implementations of the EES encryption algorithm that are used in data communications—the *("(//) stone chip* and the *TESSERA card*—do contain a public-key Key Exchange Algorithm (KEA). However, at this riting, the Key Exchange Algorithm is not part of any FIPS. Therefore, organizations that do not use Capstone or TESSERA still need to select a secure and interoperable form of key distribution. The Capstone chip is used for data communications and contains the EES algorithm (called SKIPJACK), as well as digital-signature and key-exchange functions. However, at this writing, the Key Exchange Algorithm is not part of any FIPS. Therefore, organizations that do not use Capstone (w TESSERA still need to select a secure and interoperable form of key distribution. TESS ERA is a PCMCIA card that contains a Capstone chip.

17 Vice President Al Gore, letter to Representative Maria Cantwell, July 20, 1994. See also Neil Munro, "The Key to Clipper Available to the World," *Washington Technology*, July 28.1994, pp. 1, 18.

18 For a comparison of th two export-control regimes, see U.S. General Accounting of ffice, *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), especially pp. 10-13.

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. [19] Moreover, software producers assert that several other countries do have more relaxed export controls on cryptography.

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 cryptography in the face of foreign supply and networks like the Internet that seamlessly cross national boundaries. (See the OTA report *Export Controls and Nonproliferation Policy, OTA-ISS-596,* May 1994, for a general discussion of the costs and benefits of export controls on dual-use goods.)

New licensing procedures were expected to appear in the *Federal Register* in summer 1994; they had not appeared by the time this report was completed. Changes were expected to include license reform measures 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. [20] The Secretary of State has asked encryption-product manufacturers to evaluate the impact of these reforms over the next year and provide feedback on how well they have worked, as well as recommendations for additional procedural reforms.

In the 103d Congress, legislation intended to streamline export controls and ease restrictions on mass-market computer software, hardware, and technology, including certain encryption software, was introduced by Representative Maria Cantwell (H.R. 3627) and Senator Patty Murray (S. 1846). In considering the Omnibus Export Administration Act (H.R. 3937), the 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. [21] 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 150days of enactment, regarding the current and future international market for software with encryption and the economic impact of U.S. export controls on the U.S. computer software industry. [22]

At this writing, the omnibus export administration legislation was still pending. 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 his July 20, 1994 letter to Representative Cantwell,

---

19 *The Threat @Foreign Economic Espionage to U.S. Corporations,* Hearings Before the Subcommittee on Economic and Commercial Law, House Committee on the Judiciary, Serial No. 65, 102d Cong., 2d sess., Apr. 29 and May 7, 1992.

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

21 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). For the cryptography provisions, see *Omnibus Export Administration Act of*)994, Part 1, pp. *57-58* (H.R.3937, sec. 117(c)(1)-(4)).

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

Vice President Gore assured her that the "best available resources of the federal government" would be used in conducting these studies and that the Clinton Administration will "reassess our existing export controls based on the results of these studies."[23]

Implementation of the Computer Security *Act of 1987*

The Computer Security Act of 1987 is fundamental to development of federal standards for safeguarding unclassified information, balancing national-security and other objectives in implementing security and privacy policies within the federal government, and issues concerning government control of cryptography. Moreover, review of the controversies and debate surrounding the act—and subsequent controversies over its implementation—provides background for understanding current issues concerning the EES and the DSS.

The Computer Security Act of 1987 (see text in appendix B) was a legislative response to overlapping responsibilities for computer security among several federal agencies, heightened awareness of computer security issues, and concern over how best to control information in computerized or networked form. The act established a federal government computer-security program that would protect all sensitive, but unclassified, information in federal government computer systems 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 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 Department of Commerce, and required Commerce to promulgate regulations based on NIST guidelines. 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 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. 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 (also see discussion of OMB Circular A-130 below).

The Computer Security Act gave final authority for developing government-wide standards and guidelines for unclassified, but sensitive, information and for developing government-wide training programs to NIST (then the National Bureau of Standards). In carrying out these responsibilities, NIST can draw on the substantial expertise of NSA and other relevant agencies.

Implementation of the Computer Security Act has been especially controversial regarding the roles of NIST and NSA in standards development. A 1989 memorandum of understanding (MOU) between the Director of NIST and the Director of NSA established the mechanisms of the working relationship between the two agencies in implementing the act.[24] This memorandum of understanding has been controversial. Observers—including OTA-consider that it appears to cede

[23] Vice President Al Gore, op. cit., footnote 17.

[24] Memorandum of Understanding Between the Director of the National Institute of Standards and Technology and the Director of the National Security Agency Concerning the Implementation of Public Law 100-235, Mar. 23, 1989. (See text of MOU in appendix B.)

to NSA much more authority than the act itself had granted or envisioned, especially considering the House report accompanying the legislation.[25]

The joint NIST/NSA Technical Working Group (TWG) established by the memorandum of understanding merits particular attention. The MOU authorizes NIST and NSA to establish the working group to "review and analyze issues of mutual interest pertinent to protection of systems that process sensitive or other unclassified information." Where the act had envisioned NIST calling on NSA's expertise at its discretion, the MOU's working-group mechanism involves NSA in all NIST activities related to information-security standards and technical guidelines, as well as proposed research programs that would support them.

For example, the standards-appeal mechanism set forth in the Computer Security Act allowed the President to disapprove or modify standards or guidelines developed by NIST and promulgated by the Secretary of Commerce, if he or she determined such an action to be in the public interest. Should the President disapprove or modify a standard or guideline that he or she determines will not serve the public interest, notice must be submitted to the House Committee on Government Operations and the Senate Committee on Governmental Affairs, and must be published promptly in the *Federal Register.*[26] By contrast, interagency discussions and negotiations by agency staffs under the MOU can result in delay, modification, or abandonment of proposed NIST standards activities, without notice or the benefit of oversight that is required by the appeals mechanism set forth in the Computer Security Act.

Thus, the provisions of the memorandum of understanding give NSA power to delay and/or appeal any NIST research programs involving "technical system security techniques" (such as encryption), or other technical activities that would support (or could lead to) proposed standards or guidelines that NSA would ultimately object to.[27]

NIST and NSA disagree with these conclusions. According to NIST and NSA officials who reviewed a draft of this report, NIST has retained its full authority in issuing federal information processing standards and NSA's role is merely advisory. In discussions with OTA, officials from both agencies maintained that no part of the MOU is contrary to the Computer Security Act of 1987, and that the controversy and concerns are due to "misperceptions."[28]

When OTA inquired about the MOU/TWG appeals process in particular, officials in both agencies maintained that the appeals process does not conflict with the Computer Security Act of 1987 because it concerns *proposed* research and development projects that could lead to *future* NIST standards, not *fully developed* NIST standards submitted to the Secretary of Commerce or the President.[29] In discussions with OTA, senior NIST and NSA staff stated that the appeals mechanism specified in the Computer Security Act has never been used, and pointed to this as evidence of how well the NIST/NSA relationship is working in implementing the act.[30] In discussions with OTA staff regarding a draft of this OTA report, Clinton Brooks, Special Assistant to the Director of NSA, stated that cryptography presents special

---

25 U.S. House of Representatives, *Computer Security Act of 1987-Report to Accompany H.R. 145,* H. Rept. No. 100-153, Part 1 (Committee on Science, Space, and Technology) and Part 11 (Committee on Government Operations), 100th Cong., I st sess., June 11, 1987.

26 Public Law 100-235, sec. 4. The President cannot delegate authority to disapprove or modify proposed NIST standards

27 MOU, op. cit., footnote 24, sees. 111(5)-(7).

28 OTA staff interviews with NIST and NSA officials in October 1993 and January 1994.

29 OTA staff interviews, ibid.

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

problems with respect to the Computer Security Act, and that if NSA waited until NIST announced a proposed standard to voice national security concerns, the technology would already be "out" via NIST's public standards process.[31]

However, even if implementation of the Computer Security Act of 1987, as specified in the MOU, is satisfactory to both NIST and NSA, this is not proof that it meets Congress's expectations in enacting that legislation. Moreover, chronic public suspicions of and concerns with federal safeguard standards and processes are counterproductive to federal leadership in promoting responsible use of safeguards and to public confidence in government.

It may be the case that using two executive branch agencies as the means to effect a satisfactory balance between national security and other public interests in setting safeguard standards will inevitably be limited, due to intrabranch coordination mechanisms in the National Security Council and other bodies. These natural coordination mechanisms will determine the balance between national-security interests, law-enforcement interests, and other aspects of the public interest. The process by which the executive branch chooses this balancing point may inevitably be obscure outside the executive branch. (For example, the Clinton Administration's recent cryptography policy study is classified, with no public summary.)

Public visibility into the decision process is only through its manifestations in a FIPS, in export policies and procedures, and so forth. When the consequences of these decisions are viewed by many of the public as not meeting important needs, or when the government preferred technical "solution" is not considered acceptable, a lack of visibility, credible explanation, and/or useful alternatives fosters mistrust and frustration.

Technological variety—having a number of alternatives to choose from—is important in meeting the needs of a diversity of individuals and communities. Sometimes federal safeguard standards are accepted as having broad applicability. But it is not clear that the government can--or should--develop all-purpose technical safeguard standards, or that the safeguard technologies being issued as FIPS can be made to meet the range of user needs. More open processes for determining how safeguard technologies are to be developed and/or deployed throughout society can better ensure that a variety of user needs are met equitably. If it is in the public interest to provide a wider range of technical choices than those provided by government-specified technologies (i.e., the FIPS), then vigorous academic and private-sector capabilities in safeguard technologies are required.

More open policies and processes can be used to increase equity and acceptance in implementing cryptography and other technologies. The current controversies over cryptography can be characterized in terms of tensions between the government and individuals. They center on the issue of *trust in government.* Trust is a particular issue in cases like cryptography, when national-security concerns restrict the equal sharing of information between the government and the public. Government initiatives of broad public application, formulated in secret and executed without legislation, naturally give rise to concerns over their intent and application. The process by which the EES was selected and approved was closed to those outside the executive branch. Furthermore, the institutional and procedural means by which key-escrow encryption is being deployed (such as the escrow-management procedures) continue to be developed in a closed forum.

The Clinton Administration made a start at working more closely and more openly with industry through a "Key Escrow Encryption Workshop" held at NIST on June 10, 1994. The workshop was attended by representatives of many of the leading computer hardware and software companies, as well as attendees from gov-

[31] Clinton Brooks, Special Assistant to the Director, NSA, personal communication, May 25, 1994.

ernment and academia. The proposed action plan subsequent to the NIST workshop called for the establishment of joint industry-government working groups (with NIST leadership) to: evaluate all known key-escrowing proposals according to criteria jointly developed by government and industry, hold a public seminar/workshop to discuss and document the results of this analysis, and prepare a report to be used as the basis for subsequent discussions between government officials and the private sector. Based on the discussion and industry presentations at the meeting, there was increasing interest in exploring "other" approaches to key-escrow encryption that can be implemented in software, rather than just in hardware.

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

Congressional Review of Cryptography Policy

Congress has vital, strategic roles in cryptography policy and, more generally, in safeguarding information and protecting personal privacy in a networked society. Recognizing the importance of the technology and the policies that govern its development, dissemination, and use, Congress has asked the National Research Council (NRC) to conduct a major study that would support a broad review of cryptography.

The results of the NRC study are expected to be available in 1996. But, given the speed with which the Clinton Administration is acting, information to support a congressional policy review of cryptography is out of phase with the government's implementation of key-escrow encryption. Therefore:

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

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

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:

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 re-evaluated 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 pubic visibility and accountability for government actions.

For example, many of the concerns surrounding the Escrowed Encryption Standard and the Clinton Administration's escrowed-encryption initiative, in general, 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 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.[32]

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, key-escrow encryption may already be embedded in information systems before Congress can act on the NRC report.

As part of a broad national cryptography policy, Congress may wish to periodically examine export controls on cryptography, to ensure that these continue to reflect an appropriate balance between the needs of signals intelligence and law enforcement and the needs of the public and business communities. This examination would take into account changes in foreign capabilities and foreign availability of cryptographic technologies. Information from industry on the results of licensing reforms and the executive branch study of the encryption market and export controls that was included in the 1994 export-administration legislation should provide some near-term information.

However, the scope and methodology of the export-control studies that Congress might wish to use in the future may differ from these. 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

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

The 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

[32] There are reasons why organizations and individuals might want the *option* of placing copies of cryptographic keys with third-party trustees or custodians *of their own choosing.* For example, there is growing recognition of the problems that could occur if cryptography is used in corporations without adequate key management and without override capabilities by responsible corporate officers. These problems could include data being rendered inaccessible after having been encrypted by employees who subsequently leave the company (or die).

volumes of private information about individuals (e.g., taxpayer data, health-care information, and so forth).

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

In 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:

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, and in determining the extent to which appropriated funds should be used in implementing key-escrow encryption and related technologies:

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

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. Information-security managers in federal agencies must compete for resources and support to properly implement needed safeguards. In order for their efforts to succeed, both OMB and top agency management must fully support investments in cost-effective safeguards. Given the expected increase in interagency sharing of data, interagency coordination of privacy and security policies is also necessary to ensure uniformly adequate protection.

The forthcoming revision of Appendix 111 ("Agency Security Plans") of OMB Circular A-1 30 is central to improved federal information security practices. The revision of Appendix 111 will take into account the provisions and intent of the Computer Security Act, as well as observations regarding agency security plans and practices that resulted from a series of agency visits

made by OMB, NIST, and NSA in 1992.33 In practice, there are both insufficient incentives for compliance and insufficient sanctions for noncompliance with the spirit of the Computer Security Act. (For example, agencies do develop the required security plans; however, the act does not require agencies to review them periodically or update them as technologies or circumstances change. One result of this is that, "[security of systems tends to atrophy over time unless there is a stimulus to remind agencies of its importance."[34] Another result is that agencies may not treat security as an integral component when new systems are being designed and developed.)

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

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

After the revised Appendix III of OMB Circular A-130 is issued:

OPT/O/V: Congress could assess the effectiveness of the OMB's revised guide/ines, including improvements in implementing the Computer Security Acts 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 111 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 wel*l 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:

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

---

33 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.

34 Ibid., p. I I.

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 N/ST to support its Computer Security Act responsibilities, as we// as NIST's other activities related to safeguarding *information and protecting privacy in networks.*

Regarding NIST's computer-security budget, OTA has not determined the extent to which additional funding is needed, or the extent to which additional funding would improve the overall effectiveness of NIST's information-security activities. However, in staff discussions and workshops, individuals from outside and within government repeatedly noted that NIST's security activities were not proactive and that NIST often lagged in providing useful and needed standards (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 and/or from formation of a new Information Technology Laboratory, could enhance NIST's technical capabilities, enable it to be more proactive, and hence be more useful to federal agencies and to industry.

NIST activities with respect to standards and guidelines related to cryptography are a special case, however. Increased funding alone will not be sufficient to ensure NIST's technological leadership or its fulfillment of the "balancing" role as envisioned by the Computer Security Act of 1987. With respect to cryptography, national-security constraints set forth in executive branch policy directives appear to be binding, implemented through executive branch coordinating mechanisms including those set forth in the NIST/NSA memorandum of understanding. These constraints have resulted, for example, in the closed processes by which the FIPS known as 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, clear policy guidance and oversight will be needed.

Legal Issues and Information Security

Laws evolve in the context of the mores of the culture, business practices, and technologies of the time. 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. Changes in communication and information technologies are 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 y 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, action by Congress may not be warranted now. However:

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

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.

Increased computerization and linkage of information maintained by the federal government is arguably not addressed by the Privacy Act, which approaches privacy issues on an agency-by-agency basis. To address these developments:

OPT/ON: Congress could allow each agency to address privacy concerns indivldually 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 previsions addressing the sharing and matching of data, or restructure the law overall to *track the flow of information between institutions.*

OPT/ON: 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.*

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 EU proposal, as it relates to the data subject's consent and the transfer of data to non-EU countries.

In 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.

A diversity of interests must be reflected in addressing the problem of maintaining privacy in computerized information-whether in the public or private sector:

OPTION: Congress could establish a Federal Privacy Commission.

Proposals for such a commission or board were discussed by the Office of Technology Assessment in its 1986 study of *Electronic Record Systems and Individual Privacy*. 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. Data protection boards have been instituted in several foreign countries, including Sweden, Germany, Luxembourg, France, Norway, Israel, Austria, Iceland, United Kingdom, Finland, Ireland, the Netherlands, Canada, and Australia.

The responsibilities and functions suggested for a privacy commission or data protection board are:

1. to identify privacy concerns, that is to function essentially as an alarm system for the protection of personal privacy;
2. to carry out oversight to protect the privacy interests of individuals in information-handling activities;
3. to develop and monitor the implementation of appropriate security guidelines and practices for the protection of health care information;
4. to advise and develop regulations appropriate for specific types of information systems:
5. to monitor and evaluate developments in information technology with respect to their implications for personal privacy in information; and
6. to perform a research and reporting function with respect to information privacy issues in the United States.

Debate continues as to whether such a body should serve in a regulatory or advisory capacity. In the 103d Congress, legislation (S. 1735, the Privacy Protection Act) that would establish a Privacy Protection Commission has been introduced.

Protection of Intellectual Property in the Administration of *Digital Libraries*

The availability of protected intellectual property in networked information collections, such as *digital libraries* and other digital information banks, is placing a strain on the traditional methods of protection and payment for use of intellectual property. Technologies developed for securing information might hold promise for monitoring the use of protected information, and provide a means for collecting and compensating the owners of intellectual property as well. 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 addressed these issues in *Finding a Balance: Computer Software, Intellectual Property, and the Challenge of Technological Change, OTA-TCT-527* (Washington, DC: U.S. Govern-

ment Printing Office, May 1992). The 1992 report included the following options to deal with the issue of fair use of works in electronic form:

- Congress could clarify the Copyright Act fair-use guidelines with regard to lending, resource sharing, interlibrary loan, archival and preservation copying, and copying for patron use.
- Congress could establish legislative guidance regarding fair use of works in electronic form and what constitutes *copying, reading,* and *using;*

or,

- Congress could direct the Copyright Office, with assistance from producers and users of electronic information, to develop and disseminate practical guidelines regarding these issues. [35]

With respect to questions raised concerning *multimedia* works, the 1992 OTA report suggested that:

- Congress could clarify the status of mixed-media works, with regard to their protection under copyright.[36]

During this 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:

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,

OPT/ON: 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, Congress might try a third approach. This approach would allow producer and user communities to establish common guidelines for use of copyrighted, multimedia works:

OPT/ON: 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.

With respect to rights and royalties for copyrighted works:

OPT/ON: Congress could encourage private efforts to form rights-c/earing 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 (e.g., Does it serve the *fair-use* exception? Can network technologies effectively address this question?). This might be accomplished by conducting oversight hearings, undertaking a staff analysis, and/or requesting a study from the Copyright Office.

---

[35] U.S. Congress, Office of Technology Assessment, *Finding a Balance: Computer Software, Intellectual property, and the Challenge of Technological* Change, OTA-TCT-527 (Washington, DC: U.S. Government Printing Office, May 1992), p. 35 (options 3.1, 3.2, and 3.3).

[36] Ibid., p, 36 (option 3.4).