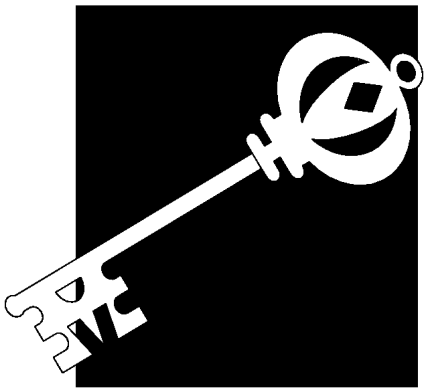
Implications for Congressional Action 4

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.