July 1995

Office of Technology Assessment
U.S. Congress

OTA REPORT SUMMARY

*

ISSUE UPDATE ON INFORMATION SECURITY AND PRIVACY IN NETWORK ENVIRONMENTS

*

As a follow-on to the September 1994 report on information security and privacy, at the request of the Senate Committee on Governmental Affairs, the Office of Technology Assessment has updated some key issues in a new background paper. In "Issue Update on Information Security and Privacy in Network Environments," OTA develops further some of its earlier options related to the effects of government policies on the private sector and to federal-agency operations to safeguard unclassified information.

OTA's Findings

As OTA's 1994 report noted, we are in transition to a society that is critically dependent on electronic information and network connectivity. The Internet now has host computers in over 85 countries; the variety of online sources of information, services, and entertainment continues to expand. Businesses' use of networks has continued to expand, and ventures to bring electronic commerce and electronic money, or "digital cash," into homes and offices are materializing rapidly. Government agencies have continued to expand both the scale and scope of their network connectivities; information technologies and networks are featured prominently in plans to make government more efficient, effective, and responsive. The transformation being brought about by networking brings with it new concerns for the security of networked information and for our ability to maintain effective privacy protections in networked environments. In contrast to the older concepts of "document" security or "computer" security, the new focus is on safeguarding the information itself as it is processed, stored, and transmitted. Responsibility for security is being shifted to the end users. Increased interactivity means that we must protect transactional privacy, while preventing fraud in electronic commerce.

OTA finds that the need for timely congressional attention to safeguarding unclassified information and protecting personal privacy is increasingly urgent. The background paper discusses a number of reasons for this conclusion, including the following:

o Congressional oversight of government information security and privacy is of utmost importance in the present time of government reform and organizational 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 historical lack of commitment on the part of top agency managements to safeguarding unclassified information. Similarly, management must ensure that safeguards are integrated when organizations streamline their operations and modernize their information systems.

o Momentum is building toward government-wide consolidation of information-security responsibilities.

Cryptography standards-development and export-control issues underlie a long history of concern over leadership and responsibility for the security of unclassified information governmentwide. Controversy over who should be in charge and who is in charge was not laid to rest after enactment of the Computer Security Act of 1987 (Public Law 100-235). Now, these concerns have been revitalized by the creation of the Security Policy Board and the Board staff proposals to centralize unclassified information-security authorities government-wide and by the prospect of new information-technology and information-security legislation in the 104th Congress.

o 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 reside within the defense/intelligence community, then vigilant oversight and clear direction will be needed. This would include assigning and funding a credible focal point (or points) for cost-effective security guidance for unclassified information. If the Computer Security Act is revisited, Congress might wish to redirect the National Institute of Standards and Technology's (NIST's) activities away from "picking technologies" for standards 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 their existing hardware and software technology investments.

o Cryptography is not arcane anymore. Cryptography also is not just a "government technology" anymore.

In its modern setting, cryptography is a fundamental safeguard with broad applications. It can be used to preserve the confidentiality of messages and files, or to provide "digital signatures" that will help speed the way to electronic commerce. The nongovernmental markets for cryptography-based safeguards have grown over the past two decades, but are still developing. Good commercial encryption technology is available in the United States and abroad. Research in cryptography is international. Markets for cryptography would also be international, except that governmental restrictions like export controls effectively segment "domestic" and "export" markets for strong encryption products. User-friendly cryptographic safeguards that are integrated into products (as opposed to those that the user has to acquire separately and add on) are still hard to come by--in part, because of export controls and other federal policies that seek to control cryptography.

o Cryptography is a technology whose time has come, but the clock is still ticking.

Because cryptography is a technology of such broad application, cryptography policies affect technological developments in the field, as well as the health and economic vitality of companies that produce or use products incorporating cryptography. Consequently, policies about cryptography exports and standards will increasingly affect both the vitality of the information technology industries and the everyday lives of most Americans. Representatives of major U.S. computer and software companies have recently reaffirmed the importance of security and privacy protections in the developing global information infrastructure. But, there are strong and serious business concerns that government interests, especially with respect to standards and export controls, could stifle commercial development and use of networks in the international arena. Given the broad public and business impacts, timely and continuing congressional oversight of these policies is crucial.

o With an increasing policy focus on domestic crime and terrorism, the availability and use of cryptography is a prominent domestic-security, law-enforcement issue.

Strong encryption is increasingly portrayed as a threat to domestic security (public safety) and a barrier to law enforcement if it is readily available for use by terrorists or criminals. Thus, export controls, intended to restrict the international availability of U.S. cryptography technology and products, are now being joined with domestic cryptography initiatives, like key-escrow encryption, that are intended to preserve U.S. law-enforcement and signals-intelligence capabilities.

o The overarching questions surrounding the Clinton Administration's escrowed-encryption initiative have not been resolved.

Public and business concerns have not been assuaged. Many of the persistent concerns surrounding the escrowed-encryption initiative focus on whether government-approved, key-escrow encryption will become mandatory for government agencies or the private sector, if non-escrowed encryption will be banned, and/or if these actions could be taken without legislation. Other concerns still focus on whether or not alternative forms of encryption that would allow private individuals and organizations the option of depositing keys (or not) with one or more third-party trustees--at their discretion--would be available. Because deployment of escrowed encryption was outpacing congressional review, OTA's 1994 options for congressional consideration included placing a hold on further deployment of escrowed encryption within the government, pending congressional review, as well as options addressing open policy implementation, and public visibility and accountability. These are still germane, especially given the National Security Agency's (NSA's) expectation of a large-scale FY96 investment in FORTEZZA cards and the likelihood that nondefense agencies will be encouraged by NSA to join in adopting FORTEZZA.

o Important questions still remain about the implementation of the Clinton Administration's escrowed encryption initiatives.

The Clinton Administration has stated that it has no plans to make escrowed encryption mandatory, or to ban other forms of encryption. But, absent legislation, these intentions are not binding. Moreover, the executive branch may soon be using escrowed-encryption technologies (e.g., in the FORTEZZA card) to safeguard--among other things--large volumes of private and proprietary information. For these reasons, OTA concluded that escrowed-encryption initiatives are by no means only an executive branch concern. They also warrant congressional attention because of the public funds that will be spent in deploying them. Moreover, negative public perceptions of the processes by which encryption standards are developed and deployed, and of the standards themselves, may erode public confidence and trust in government and, consequently, the effectiveness of federal leadership in promoting responsible safeguard use. Therefore, OTA identified options addressing the location of escrow agents, as well as criminal penalties and civil liabilities for misuse or unauthorized disclosure of escrowed key components. These topics are still germane, and the liability issues are even more timely, given recent initiatives by the international legal community and the states to develop and codify legal and liability standards.

o The Clinton Administration's key-escrow encryption initiatives (e.g., hardware implementation of NSA's "Skipjack" algorithm in Clipper and Capstone chips and the FORTEZZA card) are now being challenged by commercial alternatives.

Several companies and private-sector consortia are developing hardware and software products that employ different, commercially-accepted encryption and signature techniques yet still make provisions for legitimate law-enforcement access to encrypted material. Nevertheless, the Defense Department is continuing with plans to procure and deploy several hundred thousand FORTEZZA cards in the Defense Message System and is encouraging civilian agencies to adopt the NSA-developed technology.

o Export control issues remain.

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. 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 shown a disinclination to relax controls on robust cryptography, except perhaps for certain key-escrow encryption products. 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 and evaluation of the Administration's market study, and by encouraging a more timely, open, and productive dialogue between government and the private sector.

o The Office of Management and Budget has issued new government-wide information-security guidance.

In its 1994 report, OTA identified the need for the revised version of the security appendix (Appendix III) of the Office of Management and Budget's (OMB's) 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 OTA's view, the proposed 1995 revision to Appendix III of OMB Circular A-130 shows promise for meeting these objectives. However, OMB's approach is somewhat abstract and a significant departure from earlier, "computer security" guidance. Therefore, congressional review and oversight of OMB's revisions to Appendix III (as suggested in 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.

o Congressional review and oversight can provide additional guidance on how security activities now residing with the National Institute of Standards and Technology might best be re-focused to meet federal information-security objectives.

In addition to the Commerce Department's (i.e., NIST's) traditional responsibilities under the Computer Security Act for security standards, 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 technical assistance from the Defense Department) evaluating new information technologies to assess their security vulnerabilities and apprising agencies of these in a timely fashion. Congressional oversight targeting NIST's information-security activities towards support of OMB's new guidance (with its focus on end users and individual workstations, not mainframe computers) might enable NIST to be more effective despite scarce resources.

OVERVIEW OF THE BACKGROUND PAPER

As in the 1994 report, OTA's new background paper focuses on safeguarding unclassified information. The background paper is intended for use in conjunction with the 1994 report. For the reader's convenience, however, pertinent technical and institutional background material, drawn from that report and updated where possible, is included in the background in appendices C ("Federal Information Security and the Computer Security Act"), D ("U.S. Export Controls on Cryptography") and E ("Summary of Issues and Options from the 1994 OTA Report").

Chapter 1 of the background paper provides an introduction and policy summary. Chapter 2 gives an overview of the 1994 OTA report. Chapter 3 identifies major themes that emerged from a December 1994 OTA workshop, particularly regarding export controls and the international business environment, federal cryptography policy, and information-security "best practices." Chapter 4 provides an update on recent and ongoing cryptography, privacy, and security-policy developments and their relevance for possible congressional actions on cryptography policy and government information security

The OTA report identified policy options related to three general policy areas:

1.national cryptography policy, including federal information processing standards and export controls;

2.guidance on safeguarding unclassified information in federal agencies; and

3.legal issues and information security, including electronic commerce, privacy, and intellectual property.

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

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

1. How will we as a Nation develop and maintain the balance among traditional "national security" (and law-enforcement) objectives and other aspects of the public interest, such as economic vitality, civil liberties, and open government?

2. What are the costs of government efforts to control cryptography and who will bear them?

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

INFORMATION SECURITY AND PRIVACY

There are three main aspects of information security: confidentiality, integrity, and availability. These protect against the unauthorized disclosure, modification, or destruction of information. OTA's recent work focuses on the confidentiality and integrity of information in network environments. Confidentiality refers to the property that information is made available or disclosed only to authorized parties. Integrity refers to the property that information is changed only in a specified and authorized manner.

Privacy refers to the social balance between an individual's right to keep information confidential and the societal benefit derived from sharing information, and how this balance is codified to give individuals the means to control personal information. Confidentiality and privacy are not mutually exclusive: safeguards that help ensure confidentiality of information can be used to protect personal privacy.

INFORMATION SAFEGUARDS

OTA uses the term "safeguard" to avoid misunderstandings regarding use of the term "security," which some readers may interpret in terms of classified information, or as excluding measures to protect personal privacy. Cryptography is an important safeguard technology. Modern encryption techniques can be used to safeguard the confidentiality of the contents of a message (or a stored file). Message authentication techniques and digital signatures based on cryptography can be used to ensure the integrity of the message (that it has been received exactly as it was sent) and the authenticity of its origin (that it comes from the stated source).

CRYPTOGRAPHY

Cryptography, a field of applied mathematics/computer science, is the technique of concealing the contents of a message by a code or a cipher. Cryptography provides confidentiality through encoding, in which an arbitrary table is used to translate the text or message into its coded form, or through encipherment, in which an encryption algorithm and key are used to transform the original plaintext into the encrypted ciphertext. The original text or message is recovered from the encrypted message through the inverse operation of decryption.

Cryptographic algorithms--specific techniques for transforming the original input into a form that is unintelligible without special knowledge of some secret (closely held) information--are used to encrypt and decrypt messages, data, or other text. In modern cryptography, the secret information is the cryptographic key that "unlocks" the encrypted ciphertext and reveals the original plaintext. Key management underpins the security afforded by an cryptography-based safeguard.

KEY-ESCROWED ENCRYPTION

The Escrowed Encryption Standard, or EES, is intended for use in encrypting voice, facsimile, and computer data communicated in a telephone system. It is currently intended for voluntary use by all federal departments and agencies and their contractors to protect unclassified information; other use by the private sector is voluntary. The EES encryption algorithm, called Skipjack, is implemented in tamper-proof electronic devices, or "chips." An early implementation of Skipjack was in the "Clipper chip." The "Capstone chip" contains an implementation of Skipjack for use in computer networks. The Capstone chip is included in the FORTEZZA card being used for the Defense Message System.

The EES specifies a type of key-escrow encryption intended to allow easy decryption by law enforcement when the equivalent of a wiretap has been authorized. This is accomplished through what is called key escrowing. Each chip is programmed with a chip-specific key. A copy of this key is then split into two parts; one part is held by each of two designated "escrow agents." The EES also specifies how the Law Enforcement Access Field (LEAF) that is transmitted along with encrypted messages is created.

When intercepted communications have been encrypted using the EES, law enforcement agencies can obtain the two escrowed key components from the escrow agents. (A device identifier in the LEAF indicates which ones are needed.) The escrowed key components are then used to obtain the keys that will decrypt the intercepted communications sessions.

ORDERING INFORMATION

Congressional requests: Call OTA's Congressional and Public Affairs Office at 202-224-9241.

"Issue Update on Information Security and Privacy in Network Environments" is available from the U.S. Government Printing Office. Call GPO at 202-512-1800.

Orders placed at GPO generally take four weeks for delivery. If you need fast delivery, the Superintendent of Documents offers Federal Express service for domestic telephone orders only. The cost is an additional $8.50 per order. Inquire for bulk quantities. There is no Federal Express delivery to Post Office boxes or APO/FPO addresses.

For information about other OTA publications, a free "Catalog of Publications" is available from OTA's Publication Distribution Office. Call 202-224-8996 or e-mail pubsrequest@ota.gov or write to: Office of Technology Assessment, U.S. Congress, Washington, D.C. 20510-8025. Attn: Publication Distribution.

OTA ONLINE

Readers can access this report electronically through OTA Online, using any of the following standard Internet tools:

WWW: http://www.ota.gov

FTP: otabbs.ota.gov, login as anonymous, password is your email address, publications are in the /pub directory

Telnet: otabbs.ota.gov, login as public, password is public

Questions or comments about Internet services should be directed by email to netsupport@ota.gov

□