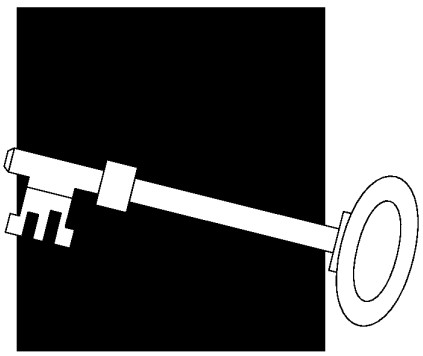
Digest of OTA Workshop Discussion 3

At the request of the Senate Committee on Governmental Affairs, the Office of Technology Assessment (OTA) held a workshop titled "Information Security and Privacy in Network Environments: What Next?" on December 6, 1994, as part of its follow-on activities after the release of the report *Information Security and Privacy in Network Environments*.[1] The purpose of the workshop was to hear the reactions from the business and network-user communities to the issues OTA had identified, as well as their priorities for any government actions. This chapter will review the workshop discussion and identify major themes that emerged, particularly regarding export controls and the business environment, federal cryptography policy, and characteristics of information-security "best practices" that are germane to consideration of government information security.

OVERVIEW

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



[1] U.S. Congress, Office of Technology Assessment, *Information Security and Privacy in Network Environments*, OTA-TCT-606 (Washington, DC: U.S. Government Printing Office, September 1994).

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

One workshop objective was to gauge participants' overall reactions to the 1994 OTA report on security and privacy. Another objective was to identify related topics that merited attention and that OTA had not already addressed (e.g., network reliability and survivability, or "corporate" privacy—see below). However, the intent of the workshop was not to rehash the issues and controversies described in the report, but rather to build on the report and push beyond it. A goal for the workshop was for participants to identify—as specifically as possible—areas ripe for congressional action.

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

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

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

OTA has identified some themes from the day's discussion that have particular significance, especially in the context of current developments, for congressional consideration of information-security issues and options identified in the 1994 OTA report. These themes, which are explored in chapter 4 of this background paper, include:

- the mismatch between the domestic and international effects of current U.S. export controls on cryptography and the needs of business and user communities in an international economy;
- the intense dissatisfaction on the part of the private sector with the lack of openness and progress in resolving cryptography-policy issues;
- the mismatch between the federal standards process for cryptography-related federal information processing standards (FIPS) and private sector needs for exportable, cost-effective safeguards;
- the mismatch between the intent of the Computer Security Act and its implementation;
- the distinction between security policies and guidelines for implementing these policies;
- the need for technological flexibility in implementing security policies; and
- the need for line management accountability for, and commitment to, good security, as opposed to "handing off" security to technology (i.e., hoping that a "technological fix" will be a cure-all).

The remainder of this chapter highlights major points and opinions expressed by the workshop participants, while attempting to convey a sense of the variety of positions propounded. It is important to note that this presentation is not intended to represent conclusions reached by the participants; moreover, the reader should not infer any general consensus, unless consensus is specifically noted.

Cryptography Policy and Export Controls

The need for reform of export controls was the number one topic at the workshop and perhaps the only area of universal agreement. Participants expressed great concern that the current controls are impeding companies' implementation of good security in worldwide operations and harming U.S.

BOX 3-1: Areas of Inquiry for Workshop

The marketplace for information safeguards (supply and demand)

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

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

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

Impacts of federal policies on business and the public

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

What should Congress do-and when?

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

firms' competitiveness in the international marketplace. More than one participant considered that what is really at stake is loss of U.S. leadership in the information technology industry. As one participant put it, the current system is "a market intervention by the government with unintended bad consequences for both government and the private sector."

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

Several participants asserted that U.S. export controls have failed at preventing the spread of cryptography, because DES- and RSA-based encryption, among others, are available outside of this country. They noted that the only "success" of the controls has been to prevent major U.S. software companies from incorporating high-quality, easy-to-use, integrated cryptography in their products. Many participants also viewed export controls as the single biggest obstacle to establishing international standards for information safeguards; one noted the peculiarity of picking a national standard and then trying to restrict its use internationally.

Participants also expressed frustration with the lack of a timely, open, and productive dialogue between government and the private sector on cryptography issues and the lack of response by

government to what dialogue has taken place.[2] Many stressed the need for a genuine, open dialogue between government and business, with recognition that business vitality is a legitimate objective. Participants noted the need for Congress to broaden the policy debate about cryptography, with more public visibility and more priority given to business needs and economic concerns. In the export control arena, Congress was seen as having an important role in getting government and the private sector to converge on some feasible middle ground (legislation would not be required, if export regulations were changed). Leadership and timeliness ("the problem won't wait") were viewed as priorities, rather than more studies and delay.

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

INFORMATION SECURITY IN THE PRIVATE SECTOR

The workshop discussion emphasized active risk acceptance by management and sound security policies as key elements of good information-security practice in the private sector. The concept of management responsibility and accountability as integral components of information security, rather than just "handing off" security to technology, was noted as very important by several participants. Sound security policies as a foundation for good practice were described as technology neutral, consistent across company cultures, minimalist, and as absolutes. Much was made of technology-neutral policies because properly applied, they do not prescribe implementations, are not easily obsoleted by changes in technology or business practices, and allow for local customization of implementations to meet operational requirements.

Information-Security Policies and "Best Practices"

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

In some of the companies represented, security policy has been refined to the point of "Thou shalt . . . not how thou shalt." Security managers are charged with developing something resembling the "Ten Commandments" of security. Importantly, these are not guidelines for implementation. Rather, they are "minimalist" directives that outline what must happen to maintain information security, but not how it must be achieved.

One of the most important aspects about these policies is that they are consistent across the entire company; regardless of the department, information-security policies are considered universally applicable. The policies have to be designed in a broad enough fashion to ensure that all company cultures will be able to comply. Broad policy outlines allow information to flow freely between company divisions without increased security risk.

The workshop discussion noted the importance of auditing security implementation against policy, not against implementation guidelines. Good security policies must be *technology neutral*, so that technology upgrades and different

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

equipment in different divisions would not affect implementation. Ensuring that policies are technology-neutral helps prevent confusing implementation techniques and tools (e.g., use of a particular type of encryption or use of a computer operating system with a certain rating) with policy objectives, and discourages "passive risk acceptance" like mandating use of a particular technology. This also allows for flexibility and customization.

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

Availability of Secure Products

The question of the availability of secure products generated some disagreement over whether the market works or, at least, the extent to which it does and does not work. As described above, there was consensus that export controls and other government policies that segmented market demand were undesirable interventions. Though the federal government can use its purchasing power to significantly influence the market, most participants felt that this sort of market intervention would not be beneficial overall. Many felt the market will develop security standards and secure systems if left to its own devices; others took issue with this position.

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

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

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

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

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

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

Training

Most security managers participating in the workshop viewed training as vital to any successful information-security policy. Lack of training leads to simple errors potentially capable of defeating any good security system—for example, employees who write their passwords on paper and tape it to their computers. Several participants knew of companies that have fallen into the technology trap and have designed excellent computer security systems without sufficiently emphasizing training.

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

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

Common Themes

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

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

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

Domestic and International Privacy Issues

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

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

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

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

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

Proprietary Information and Intellectual Property

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

---

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

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

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

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

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

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

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

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

---

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

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

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

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

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

Views on Congressional Action

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

Cryptography Policy and Export Controls

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

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

Possible Congressional Actions:

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

Federal Standards and Open Dialogue

There was a general consensus on the need for ground rules and standards for safeguarding information, but much disagreement on how this should be done. There was sentiment that leadership is needed from the government on these issues. However, many participants did not think the government should or could set these standards. Many felt the information-policy branches of the government are unable to respond adequately to the current leadership vacuum; therefore, they felt that government should either establish a more effective policy system and open a constructive dialogue with industry or leave the problem to industry.

The lack of public dialogue, visibility, and accountability, particularly demonstrated by the introduction of the Clipper chip and promulgation of the EES, is a constant source of anger for both industry representatives and public interest groups.

There were many concerns and frustrations about the role of the National Security Agency. Several individuals felt that dialogue on information policy is paralyzed because NSA is not allowing open discussion nor responding in any tangible way to the needs of industry. Many par-

ticipants suggested that this country desperately needs a new vision of national security that incorporates economic vitality. They consider that business strength is not part of NSA's notion of "national security," so it is not part of their mission. As one participant put it, "saying that 'we all have to be losers' on national security grounds is perverse industrial policy."

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

Possible Congressional Actions:

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

Information Security in Federal Agencies

Participants suggested that there needs to be more emphasis on securing unclassified information and that there needs to be leadership. According to some participants: the government should get "its house in order" in the civilian agencies; few companies are so badly managed as government agencies; senior managers are unaware of responsibilities and untrained. As a result, participants noted, the architecture and policy constructs of the international information infrastructure are being developed right now, but these are "being left to the technologists" due to lack of leadership.

Several felt that there has been overemphasis on cryptography, to the exclusion of management; severe problems like errors and dishonest employees are not addressed by this "technology" focus. Participants considered that the real issue is *management*; technology sloganism along the lines of "buy C2 [a computer security rating] and you're OK" is not enough. According to participants, existing policies [e.g., the previous version of OMB Circular A-130, Appendix III] attempt to mandate cost-based models, but the implementation is ineffective. For example, after the Computer Security Act, NIST should have been in a position to help agencies, but this never happened due to lack of resources. Civil agencies lack resources, then choose to invest in new applications rather than spend on security. This is understandable when the observation that "nothing happens"—that is, no security incidents are detected—is an indicator of good security. Participants observed that, if inspectors general of agencies are perceived as neither rewarding or punishing, users get mixed signals and conclude that there is a mismatch between security postures and management commitment to security implementation.

There was widespread support for the Computer Security Act of 1987, but universal frustration with its implementation. NIST, the designated lead agency for security standards and guidelines, was described as underfunded and extremely slow. There was also a general recognition that people had been complaining about NIST for a while, but nothing has happened as a result of these complaints.

Possible Congressional Actions:

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

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

Privacy

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

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

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

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