Chapter 5

Improving Information Security

CONTENTS

Box

Tables

Chapter 5

Improving Information Security

FINDINGS

- The needs of institutional users are changing, expanding gradually and incrementally, as technology makes practical a broader range of applications of information safeguards. The current trend in user activities is toward controlling access to systems, linking transactions with particular individuals and authorizations, and verifying message accuracy.
- Users in civil agencies and the private sector have diverse needs to safeguard their computer and communications systems, even within any one Federal agency or industry. Organizations differ in their needs, perceptions, and attitudes towards information security, and see different incentives or mandates to secure information systems. Differences in their concerns for vulnerabilities, risks, and adversaries are probably greatest between Government intelligence agencies and other users.
- It is unclear whether anyone agency can specify and design one or a few safeguards for a wide range of users, and particularly questionable for the National Security Agency due to its propensity for secretiveness and its focus on protecting against foreign intelligence adversaries.
- Cryptography underlies some powerful safeguards that have broad application, not just for national security needs, but also for an expanding number of commercial needs, such as to ensure the integrity of electronic information and reduce the costs of routine business transactions. Advances in cryptography have stimulated new nondefense applications of the technology.
- Federal standards and guidelines have a leveraging effect on the private sector, especially in areas related to cryptography.
- It is not clear how motivated the nondefense private sector will be to use some safeguards, such as secure telephones or trusted computers, particularly if these are not easy to use and cost-effective in business applications.

INTRODUCTION

The preceding chapters illustrate the various vulnerabilities of computer and communications systems and the range of technologies that are becoming available to safeguard information in these systems. They also introduce the notion of a spectrum of adversaries, differing widely in available resources (time, money, equipment, and specialized knowledge), against whom these systems may need to be protected. This chapter examines the perceived needs of various users—defense and civilian agencies of the Federal Government, financial and other private sector users—as indicated by the actions they are taking to safeguard their domestic and international operations. It also points out some of the diversity in their perceived needs for safeguards, both among users in the private sector and, particularly, between users in intelligence agencies and others.

The level of users' activity toward safeguarding electronic information is growing. Various factors are contributing to this interest. These factors range from wanting to improve business operations, including the reduction of potential theft and human errors, to streamlining business transactions and adhering to industry standards of due care and, in some cases, to requirements imposed by emerging Federal policies. Federal policies, for example, will influence the actions of some banks and defense contractors. No individual factor is recognized as singularly prominent in driving the use of safeguards.

Instead, business uses of electronic safeguards are in a transition phase as users continue to define their needs and as technical standards are developed, and as Federal policies and agency roles stabilize further. A number of factors have complicated the situation, however. Among these is the question of the influence of the National Bureau of Standards or the National Security Agency in setting standards for information security safeguards, and users' perceptions of the prospective reach of Federal policies requiring safeguards for unclassified information. (See ch. 6.)

One important turning point appears to have been reached in that users are now better able to distinguish between the protections provided, or not provided, by different forms of safeguards and their alignment with specific needs. Users tend to be concerned with one or more of three main objectives in seeking information safeguards: preventing unauthorized disclosure; maintaining the integrity of electronic information; and ensuring continuity of service. The needs of different communities of users vary widely and these needs are often critical for one of these objectives and less important, or nonexistent, for others. For some users there is concern for all three objectives.

In spite of the difficulty in distinguishing between users according to their objectives for information security, some cautious observations can be made. One of these is that a critical need for some users, such as intelligence agencies, is to prevent unauthorized disclosure. Most businesses and civilian agencies are particularly dependent on the integrity of certain of their electronic information, and many of these are also concerned about unauthorized disclosure. And, for some users, such as those responsible for public safety (air traffic control) and many financial services, there is an important, if not critical, need for continuity of service. Observations concerning users' objectives are important because Federal policy that is misaligned with users' needs can create significant tensions.

Government agencies' and private sector needs for information security include capabilities for authenticating the origin and integrity of messages, and for verifying the identities and authorizations of system users. The Department of the Treasury and the Federal Reserve System, for example, electronically transfer huge amounts of money every working day and, with commercial banks, are providing leadership in developing and using safeguards with these types of capabilities.

Users' needs for safeguards are by no means confined to the financial community. The use of safeguards for securing electronic information is being adopted by users in industries ranging from automobile manufacturing to grocery businesses. However, private sector needs and Government national security concerns are not identical. They differ in their perceptions of the levels of adversaries, the consequences of exploitation, and their organizational motivations and decision rules for protecting information and investing in safeguard technology.[1]

In addition, private sector demand for safeguards is growing, as is its ability to produce them, as noted in chapter 4. Users tend to make selected use of a broader range of new technologies for safeguarding information that prove cost-effective or are otherwise important for business reasons. Interestingly, many of the emerging commercial uses of message integrity (authentication) techniques, e.g., for

[1] Administrative and technical safeguards, as well as organizational policies for information safeguards, are also important for safeguarding electronic information, as noted in ch. 4.

cost-reduction purposes, make use of the same cryptographic techniques used to improve the confidentiality of electronic information. Often, however, the commercial motivations for employing these techniques are unconcerned with preventing unauthorized information disclosure or protecting national security.

What emerges is a sense that although generalizations of aggregate users' needs are useful, individual users tend to have significant diversity among them. Even within one user community, such as the banking industry, there can be considerable diversity of needs, depending on size, location, operations, clients, and numbers of branches and correspondents.

This diversity of needs raises questions with regard to the proper role of the Federal Government in meeting private sector needs and the extent to which any one Federal agency can reasonably be expected to meet the safeguard needs of all users. Such a task would require an agency to interact openly and continually with a diverse public. The intensity and openness of interaction would require significant adaptation in the operations of an agency such as DoD's National Security Agency (NSA).[2] Without a full appreciation of users' needs, there is significant risk of premature or "off-target technology standardization or imposing DoD restrictions that are unacceptable to users. At the same time, safeguards that do not meet users' needs-even those that are federally imposed—are not likely to be applied widely and may distort market forces.

The users themselves are also likely to be important in shaping information safeguards. The influence of major international business users on information security standards is only beginning to be felt, but is likely to be significant in the long term. These users can be expected to demand safeguards that integrate well into their business operations in terms, for example, of being inexpensive, exportable, interoperable, and politically acceptable in the many countries in which the firms do business. Their influence is already beginning to be felt through communities of industry users, such as international banking, transportation, and manufacturing.

OTA analyzed survey data to gain insights into the influence of Federal policies and standards on users' and vendors' actions. Although the effects of National Security Decision Directive 145 (NSDD-145), issued in 1984, were still evolving, there were indications, as of late 1986, that the impact of this policy had not been widely felt on nongovernment users' actions. For example, about three-fourths of the nongovernment respondents to an OTA survey question, and 46 percent of the nongovernment respondents to a separate Ernst & Whinney survey, indicated that this policy had no impact on their organizations' actions toward safeguarding unclassified information.[3]

Moreover, OTA's research has found that some large firms feel that, in general, Federal guidelines and assistance programs have not significantly or directly contributed to their information security efforts.[4] Moreover, data from Ernst & Whinney's computer security survey in 1986 shows that, of 474 respondents, two-thirds said that none of their organization's information and computer security expertise came directly from Government-sponsored assistance programs, conferences, or training programs. On average, according to estimates by both government and nongovernment respondents, only 7 percent of their orga-

[2]See, for example, " 'Advice Most Needed . . . ' The Assessment and Advice Effort, " Deborah M. Claxton, DoD. Presented at the Ninth National Computer Security Conference, Gaithersburg, MD, Sept. 18, 1986.

[3]Of 26 computer audit directors from Fortune 100 firms surveyed for OTA in October 1986, Ernst & Whinney found that 17 individuals (74 percent of the 23 answering this question) said that NSDD-145 had had "no" impact on their firms' safeguarding of unclassified information, four saidNSDD-145 had had "very little" impact, and two said the directive had had "some" impact.

Results are reported in OTA contractor report, "OTA Computer Security Survey," Ernst& Whinney, Nov. 7, 1986. Ernst & Whinney included many questions from the OTA survey in a survey it conducted at the Computer Security Institute Conference in November 1986. The raw data from this Ernest & Whinney survey indicated that, of 364 nongovernment respondents, 46% said that NSDD-145 had had "no' impact, 27% "'very little" impact, 21% "some" impact, and 6% "great" impact (see table 9). Ernest & Whinney has permitted OTA to use the *raw* data from this survey.

[4]OTA survey, October 1986, op. cit.

nizations' information and computer security expertise came directly from government programs.[5]

Vendors of information security products are especially, and understandably, sensitive to Government policies and standards that influence the use and choice of safeguards among Government agencies and businesses. The relatively small markets for many types of safeguards make any influences on consumption of these products particularly important.

The following sections examine the range of users' motivations for using safeguard technologies to protect unclassified information and spotlight what users are doing to meet their objectives. They illustrate some of the main objectives of users for safeguarding electronic information, ranging from national security to economic self-interest and the need to comply with established business practices.

For the purposes of this report, user objectives and actions are grouped into two categories:

1. those related to national security, which include a number of Federal agency actions; and
2. other Government and private sector actions not directly related to national security.

The latter category includes Federal agency actions to protect financial transactions. Attention often focuses on cryptography because it is central to many powerful safeguard techniques and because the course of technological development in cryptography-based safeguards has been so tightly meshed with Federal policies.

[5]This data is from Ernst & Whinney's survey administered at the Computer Security Institute Conference on Nov. 17-20. 1986.

NATIONAL SECURITY OBJECTIVES AND PROGRAMS

Background

Traditionally, national security objectives have guided the development and use of effective information security techniques. DoD has been responsible for safeguarding classified information transmitted, stored, or processed in communications and computer systems. Recently, through NSDD-145, DoD's authority has been expanded to include protecting systems containing certain unclassified information in civilian agencies and the private sector. (See ch. 6.) This includes Government and Government-derived economic, human, financial, technological, and law enforcement information, as well as personal or proprietary information provided to the Federal Government.

Federal Telecommunications Protection Programs

Most Federal agencies have adopted some policy to protect the security of the information they collect. Issues relating to the security of Federal information systems were examined in an earlier OTA report, *Federal Government Information Technology: Management, Security, and Congressional Oversight.*[6] This section describes selected programs to protect information systems.[7]

Commercial Carrier Protection Program.– This program, begun prior to the issuance of Presidential Directive/National Security Council 24 (PD/NSC-24), involves the Nation's major telecommunications carriers. In late 1977, *The New York Times,* among other newspapers, reported that President Carter had approved a broad protection program that included rout-

[6]OTA-CIT-297, February 1986. Chapter 4 of this report surveys the security of unclassified information systems within the Federal Government.

[7]Part of this section is based on material taken from chapter IV of OTA contractor report, "Vulnerabilities of Public Telecommunications Systems to Unauthorized Access, " Information Security, Inc., November 1986.

ing nearly all Government telephone messages in three cities (Washington, D. C., New York, and San Francisco) through underground cable rather than over more vulnerable radio circuits.[8] At the same time, research was accelerated to improve telephone security with the long-haul, terrestrial commercial carriers. As a result, entire radio channels are now protected between switching stations in the three cities. After the technology was developed to protect the microwave radio systems, the Government began to require protected service in civil and defense agencies' communications procurements. (See ch. 6 for a description of the evolution of these communications security programs.)

Currently, 450 microwave radio channels carrying more than 1 million voice and data circuits are protected. More than 1 million sensitive telephone calls are protected each day and NSA expects that almost 2 million circuits will be protected in 1988. Although this program was prompted by defense concerns for safeguarding DoD contractor communications, defense and non-defense protection requirements were aggregated for efficient bulk or network-level protection.[9]

Secure Voice Programs. -As reported by *The New York Times* in late 1977, the Executive Secure Voice Network program was initiated to provide 100 selected Government executives and surveillance targets[10] with a total of 250 secure voice terminals at a cost of $35,000 each. The equipment, intended to secure classified information up to Top Secret Compartmented, used narrowband, dial-up telephone lines. It had a mode for automatic keying based on secure distribution of the classified cryptographic key from a secure (electronic) key distribution center. NSA funded deployment of the network. [11]

A successor, the Secure Telephone Unit II (STU-II), was developed by NSA in the early 1980s for protecting classified information up to Top Secret Compartmented, depending on the classification of the cryptographic key. The STU-II program also implemented a secure key distribution center.[12] STU-II phones, which cost about $12,000 each, operate over ordinary telephone circuits and could be purchased until December 1986. The General Services Administration (GSA) was made system manager to support the purchase, operation, and maintenance of more than 3,000 STU-II phones by civilian agencies, according to NSA.[13]

The new STU-III program was announced by NSA in March 1985, subsequent to NSDD-145. STU-III units will be produced for use by Federal agencies, Government contractors, and certain other private sector firms. NSA, which will manage the cryptographic keys, plans to produce 500,000 phones at $2,000 each. As of late 1986, orders for 49,640 units (to be delivered in late 1987) had been placed, with options for additional units. The average unit price was $3,827. As of January 1987, 37,116 of the initial orders were for defense agencies and 9,675 for nondefense agencies. About 200 STU-III phones had been ordered by Government contractors.]' The STU-III program is discussed in more detail later in this chapter.

[8]"Carter Approves Plan to Combat Phones by Other Nations, " New *York Times, Nov. 20, 1977,* p. 34.

[9]Harold E. Daniels, NSA S-0033, Feb. 12, 1987, p. 2 of Enclosure 3.

[10]Information Security, Inc., "Vulnerabilities of Public Telecommunications Systems to Unauthorized Access, OTA contractor report, reference 12, November 1986.

[11]NSA S-0033, op. cit., p. 2 of Enclosure 3.

[12]In the STU-II Program, key distribution for the civil agencies is handled by GSA Key Distribution Centers. GSA is the overall Government manager for the Federal Secure Telephone System (STU-II phones), serving some 65 to 70 agencies and managing their STU-I I installations, maintenance, system management, and procurement. In the successor STU-I II Program, the NSA will do all keying through the NSA Key Management Center. Source: Discussion between OTA staff and GSA Special Programs Division and Electronic Services Division staff, Oct. 8,1986. The STU-III phones will be procured commercially; plans for maintenance and servicing have not yet been announced.

Under the FSTS Systems Manager charter from NSA, GSA supports FSTS operations governmentwide, including operating the FSTS Key Distribution Centers (KDCs). It serves users in the defense and civil agencies, as well as some private consultants to the Government. Source: Harold E. Daniels, Jr., NSA S-0033-87, Feb. 12, 1987, p. 3 of Enclosure 3.

[13]NSA continues to provide a portion of the cost to sustain GSA's systems manager responsibilities.

[14]NSA S-0033-87, op. cit.

Government Procurements

GSA issued the first public competitive procurement for private line protected service between Washington, D.C. and San Francisco in 1980. This set the precedent for numerous subsequent procurements, particularly in having the carriers provide protection. A turnkey system was provided by RCA American with integrated protection for about a 5-percent cost premium over the unprotected service. The 5-year contract cost about $15 million to protect 312 circuits.

More recently, the Defense Communications Agency (DCA) awarded a major contract to AT&T for a nationwide, all-digital service called the Defense Commercial Telecommunications Network (DCTN). The 10-year, $1-billion program provides optional encrypted service among 161 locations, with link encryptors integrated into the carrier's earth stations. DCTN is designed to be flexible enough to allow for changes in technology and in customer requirements over the 10-year period. It also permits the use of video teleconferencing, switched voice, Autovon, and a wide range of data modes. DCA has also awarded a $100-million contract to Hawaii Telephone for a secure turnkey network called the OAHU Telephone System.

The largest program to date is for GSA's Federal Telecommunications Service-2000 (FTS-2000), a commercial communications service for Federal agencies.[15] FTS-2000 will eventually replace GSA's current long-distance telephone system, which has some 1.3 million subscribers who total 1.5 billion call-minutes per year.

FTS-2000 differs from the current system in that it will procure telecommunications services rather than leased facilities. FTS-2000 includes contractor-provided security features. GSA expects to award a contract by late 1987, with services to begin in 1988 at an expected first-year cost of $350 million. FTS-2000 is intended to be compatible with the evolving all-digital systems, generally referred to as the Integrated Services Digital Network (ISDN).

In its draft request for proposal, GSA required four specific security features for FTS-2000. The system has to:[16]

1. protect terrestrial radio systems in certain geographic areas and the communications links of any satellite system used to provide services;
2. provide protection from loss, degradation, or alteration by intrusion for the portion of those databases and information processing systems that are critical for continued reliable operation;
3. protect common channel signaling paths by NSA-endorsed encryption equipment or by other approved, nonencrypted forms of protection (e.g., fiber, cable); and
4. provide the capability to encrypt the command and control link of any-spacecraft launched after June 17, 1990.

FTS-2000 is expected to significantly affect communications security in the private sector, according to National Security Agency officials. It is expected to stimulate the development of link encryptors, protected services, signaling channel protection, and command-and-control encryption for satellites, thereby making these features more readily available to the private sector and at lower prices.

Carrier Protection Services

Microwave radio systems began to be used to augment the existing AT&T cable infrastructure in the 1950s. By the 1960s they had become the dominant long-distance transmission medium. New companies providing communications services in the 1970s typically installed microwave circuits or used new communication satellite technology. In the 1980s, optic fiber has become the favored medium for new point-to-point circuits, while satellite is still preferred for many broadcast applications.

[15] Information Securities, Inc., OTA contractor report, "Vulnerabilities of Public Telecommunications Systems to Unauthorized Access," November 1986, and OTA staff discussions with GSA officials August 1986.

[16] Information Securities, Inc., OTA contractor report, "Vulnerabilities of Public Telecommunications Systems to Unauthorized Access," November 1986, reference 19.

(See ch. 3 for a discussion of the vulnerabilities of these systems.)

The protected services offered by the communications common carriers stem in large part from Government efforts in the 1970s to develop and install safeguards for microwave circuits. Satellite carriers also developed various means of encrypting transmissions relayed by their geostationary satellites. These efforts were sparked by Government encryption requirements and, in one instance, by anticipated commercial demand. Several major carriers are developing various additional services, including protected private-line services, microwave and satellite link encryption, and all-fiber net works.

At present, the interexchange carriers have announced no plans to directly protect the proposed Integrated Services Digital Network. Standards for this future network have not been decided. Nor has it been determined whether U.S. or European designs will be used. A large number of switch and PBX manufacturers are committed to providing ISDN-compatible interfaces to their customers. Users wishing to secure ISDN service can follow one of two strategies: demand protection from each carrier for the portion of the circuit provided by that carrier (link protection) or encrypt their own communications from end to end.[17] End-to-end encryption would be under the user's control, with the encryption taking place in the user's PBX, in the carrier's Centrex service, or at the ISDN interface.

DoD Programs Under NSDD-145

DoD Outreach Programs. -According to National Security Decision Directive 145 (NSDD-145), the Secretary of Defense is the executive agent for telecommunications and information systems security, with the national manager being the Director of the National Security Agency (NSA), as discussed in chapter 6. Therefore, most programs initiated under NSDD-145 are under the auspices of the National Telecommunications and Information Systems Security Committee (NTISSC), which is chaired by an assistant secretary of defense. According to NSA, the approach being taken is to focus on the national interest in addressing information security, and to develop integrated and coordinated safeguards for classified and unclassified information rather than to segregate information security concerns into defense and civilian needs. By developing integrated standards for defense and civilian agencies and for private sector use, NSA hopes to lower the cost of safeguard products and, thereby, increase their use.[18] OTA was unable to obtain an unclassified summary of all programs initiated by DoD under NSDD-145.

The following summarizes selected DoD programs under NSDD-145 that affect civil agencies and the private sector. It is based on materials provided by NTISSC.[19]

- *Civil Agency Customer Support:* A branch within the National Computer Security Center (NCSC) was organized in 1986 to provide services to civil agencies and departments, including:
  - —onsite security enhancement reviews to identify threats and vulnerabilities, and provide recommendations for improvements;
  - —technical consultations and/or one-time review visits (less detailed reviews);
  - —assistance in preparing proposals for trusted computer system procurements;
  - —assistance in drafting security policies; and
  - –briefings on computer security, NCSC, and other related topics.
- *Trusted Computer System Training:*. NSA issued the *Department of Defense Trusted Computer Systems Evaluation Criteria, also* known as the "Orange Book, " to all Federal agencies and departments in No-

[17] As of late 1986, DoD appeared to be favoring a link encryption strategy. Commercial users, who do not have control over the circuit infrastructure, may be more likely to choose end-to-end encryption.

[18] Harold E. Daniels, Jr., NSA S-0040-87, Feb. 20,1987, Enclosure A.

[19] Letter from Donald C. Latham to OTA, NTISSC-089/86, Nov. 7, 1986.

vember 1985 for consideration as a national standard. To aid this review, NCSC presented briefings and tutorials to more than 70 Federal agencies.

- *Special Assistant for Civil and Private Sector Programs:* To fulfill its obligations under NSDD-145, NCSC, in the summer of 1986, created a senior-level position for a person to help define future directions and strategies for NCSC interactions with the civilian agencies and the private sector.
- *Computer Security Training for Civil Agencies: NCSC* has organized and is giving courses in computer security to Federal employees of the civilian agencies. The one-week courses are given twice a year and are open to all Federal agencies. Also, NCSC has initiated an annual computer security training seminar to allow computer security trainers throughout the Federal Government to exchange information on effective methods.

Data Encryption Standard (DES) Endorsement Program. -Launched by NSA in October 1982 (before NSDD-145), this program is designed to test and endorse equipment using DES to protect national security-related telecommunications in compliance with Federal Standard 1027.[20] Under the program, vendors wishing to supply endorsed cryptographic products for unclassified use by Government agencies and contractors submit their DES components (electronic devices) to the National Bureau of Standards (NBS), which validates the component correct implementation of the DES algorithm. NSA then determines whether the product meets all other Federal requirements for endorsement and certification.

By October 1986, 32 families of equipment (17 voice, 14 data, and 1 file encryptor), totaling some 400 models, had been formally endorsed.[21] These products are available to protect unclassified Government information and all levels of sensitive private sector information.

NSA announced in 1986 that it would terminate the DES Endorsement Program in 1988 in favor of the Commercial Communications Security Endorsement Program (see below)." According to NSA, the change was a result of several factors, including the fact that DES has been a widely applied public algorithm for 15 years and, as such, a worthwhile target for adversaries. Therefore, NSA considers it prudent for DES to be phased out over time.[22]

The announcement has led some users to infer that DES is now unsound and, reportedly, to delay adopting safeguards because of confusion over the longevity of DES and the roles of NSA and NBS in setting standards for cryptographic algorithms.[24] In particular, the American Bankers Association, which says that the U.S. banking industry had already invested years of work and several million dollars in DES-based equipment, spent 16 months (from October 1985 to February 1987) educating NSA about their business needs. ABA spokesmen have said that, "Our industry has lost momentum in adopting improved security technology, and it remains to be seen if we can overcome the damage that has been done to the perceived security of DES-based techniques. "[25]

Commercial Communications Security (COMSEC) Development Programs.–One of NSA's stated goals is to "make high-quality, low-cost cryptography available to qualified communications manufacturers for embedding in their

[20] Telecommunications: General Security Requirements for Equipment Using the Data Encryption Standard, " Apr. 14, 1982.

[21] Information Security, Inc., "Vulnerabilities of Public Telecommunications Systems to Unauthorized Access, " OTA contractor report, November 1986, ref 14.

[22] According to NSA, DES products endorsed prior to Jan. 1, 1988 can be used indefinitely. Harold. E. Daniels, NSA S-0033-87, Feb. 12, 1987, p. 4of Enclosure 3.

[24] Peter Hager: "NSA Plan to Replace DES Draws Criticism, " *Government Computer News,* May 9, 1986. Cheryl W. Helsing, Testimony on Behalf of the American Bankers Association before the House Committee on Science, Space and Technology, Feb. 26, 1987,

[25] Ibid., Cheryl W. Helsing.

products. "[26] According to NSA, "qualified' manufacturers of such products must meet four basic criteria.[27~] These are:

1. The firm must not be under foreign ownership, control, or influence, as prescribed by the Defense Investigative Service (DIS).
2. The firm must have or obtain a DIS facility clearance because the cryptographic design information is classified even though the resultant products are not.
3. The product host in which the firm proposes to embed cryptography must, in NSA's estimation, make obvious market sense.
4. The company must demonstrate that it can produce products that meet or exceed NSA's minimum standards of quality and reliability y.

NSA has established two programs to achieve its goal: one to develop the host products and the other to develop the embeddable cryptographic modules. The first, called the Commercial Communications Security Endorsement Program (CCEP), is a "business method" partnership between NSA and U.S. firms to develop a variety of secure products, such as personal computers, radios, and local area networks. The approach pairs NSA's cryptographic expertise, as embodied in embeddable modules that implement secret NSA cryptographic algorithms, with vendors' investments to develop host products that incorporate the modules. According to NSA, the industry partner then sells a "value-added" product. As of November 1986, NSA had about 40 such partnerships arranged through memoranda of understanding." The first CCEP secure system was available in 1986. [29]

The second program is another joint NSA/industry venture called the Development Center for Embedded COMSEC Products (DCECP). Eleven large U.S. corporations–Harris, Motorola, RCA, Rockwell International, Hughes Aircraft, GTE, AT&T Technologies, IBM, Xerox, Intel, and Honeywell—have joined with NSA to produce modules for use in products to be developed for the commercial COMSEC program. According to NSA, these corporations were chosen based on their expertise in making selected telecommunication products. Each firm will manufacture one or more types of the NSA modules after NSA has evaluated and approved them. Each manufacturer may embed its modules within its own host equipment, a personal computer or a secure telephone, for example, and/or sell the modules to other "qualified" host equipment manufacturers. Commercial divisions in each corporation are assisting in the design and review of the standard modules to ensure that they can be used in a wide variety of commercial equipment.[30]

In addition to the list of endorsed DES products mentioned above, NSA also maintains lists of endorsed information security products and potential products. The information security products on these lists have been evaluated and endorsed by NSA as having met standards or requirements for use by the Government and its contractors to protect classified or unclassified, but sensitive information. The endorsement certifies cryptographic systems as having met NSA security specifications for a specified level of security. Items on their potential list are under development. As of December 1, 1986, 14 firms and some 30

[26]NSA Press Release for Development Center for Embedded CO N! SEC Products, Jan. 10, 1986 (enclosure in letter from D. Latham to OTA, Nov. 7, 1986).

[27]Letter from Harry Daniels to OTA, Feb. 12, 1987, p. 5 of Enclosure 3. According to NSA, these criteria are prudent and not overly burdensome to potential participants. However, the requirements for security clearances from the Defense Investigative Services might be seen as burdensome by some firms, especially smaller firms that do not ordinarily need them for their personnel.

[29]"Commercial COMSEC Endorsement Program," enclosure in letter to OTA from Donald Latham, Nov. i', 1986.

[29]Information Security, Inc., "Vulnerabilities of Public Telecommunications Systems to Unauthorized Access, OTA contractor report, November 1986, p. 38.

[30]Ibid., and NSA S-0033-87, p. 6 of Enclosure 3.

cryptographic products were on the endorsed list; about 30 firms and products were on the potential list.

Further, NSA lists computer systems, software, or components that have been evaluated according to DoD's evaluation criteria for trusted computer systems. NSA also lists companies that provide communications encryption services and equipment evaluated according to the National TEMPEST Standard (NACSIM 5100A).

Standard NSA Product Line of Cryptographic Modules.–The "modules" being developed under the DCECP are sets of integrated circuits or printed wiring boards incorporating these "chip sets." According to NSA, each module is a general-purpose cryptographic device for digital data. The standard modules are designed to be transparent to the user, with a flexible, microprocessor-compatible interface and control structure.[31] The standard module approach is intended by NSA to foster development of interoperable secure systems, using well-defined interfaces and common design features throughout the family of standard modules.

In its announcement for the standard Type 1 product line intended for classified digital information, NSA noted such additional features as tamper resistance, electronic and/or over-the-air re-keying, and enhanced transmission-error detection. There are four Type 1 modules, for classified applications in three general bandwidths. There also will be three Type 2 modules, intended for unclassified, but sensitive applications.

Names, specifications, and applications of the Type 1 modules are as follows:

- *WINDSTER:* Data rate up to 200 kb/s; 9 cryptographic modes; suitable for handheld radios, pocket pagers, and telephones. (Note: A lower performance module called INDICTOR is also available.)
- *TEPACHE:* Data rate up to 10 Mb/s; 6 cryptographic modes; suitable for minicomputers, modems, local area networks, and word processors.
- *FORESEE:* Data rate up to 20 Mb/s; 7 cryptographic modes; suitable for satellite links, microwave links, fiber optic links, and mainframe computers.

Type 2 modules, which will be available at an unspecified future date, have been given the names EDGE SHOT (same data rate as WINDSTER), BULLETPROOF (same data rate as TEPACHE), and BRUSHSTROKE (same data rate as FORESEE). Types 1 and 2 modules are intended to be interoperable within each bandwidth.[32] NSA plans to key Type 1 modules through a secure key management system. It is not clear whether private firms that choose to use Type 2 modules will be able to control key generation independently of NSA.

NSA notes that the modules are designed to perform more system security functions than if they contained just a "naked" key generator chip and to leave fewer security functions for the host vendor to add on. However, to accommodate a wider range of commercial host products, NSA has an alternative commercial Type 2 "naked" key generator chip available to potential host vendors. Type 2 modules will be made available to qualified firms that have a memorandum of understanding with NSA, to firms under contract with NSA or other Government agencies to develop a cryptographic product, to Government agencies doing cryptographic development, and to certain other firms approved on a case-by-case basis.[33]

Some users have expressed concerns that the embedded cryptography will not be readily compatible with their existing equipment and operations, and others note that the change is damaging to manufacturers of DES equip-

[31] "Off the Shelf Information Security Products: A Family of User-Friendly Modules for Embedding Within a Wide Range of Telecommunication Systems, NSA; enclosure to letter from D. Latham to OTA, Nov. 7, 1986.

[32] Information on Types 1 and Type 2 modules were provided by NSA at a meeting of the IEEE Subcommittee on Privacy, June 18, 1986.

[33] Harold E. Daniels, Jr., NSA S-0033-87, Feb. 12, 1987, pp. 8-9 of Enclosure 3.

ment. To ease the transition, NSA had offered to work with manufacturers of the Data Encryption Standard (DES) components and develop pin-for-pin replaceable circuits using the new NSA algorithms, so that equipment manufacturers' investments in product designs would not be lost. According to NSA, none of the DES component manufacturers expressed interest in this plan. [34]

STU-III Program.-NSA initiated the Secure Telephone Unit III (STU-III) program in 1984 to develop a new generation of secure telephone equipment using classified NSA algorithms (but not the standard modules being developed under the DCECP program). NSA intends that the STU-III program serve all Government agencies and private companies that require telephone security. NSA-sponsored studies have estimated a market for 2 million units, with DoD being the largest single buyer. Market studies by vendors also indicate potential sales of 1 million to 2 million units to the private sector,[35] although these conclusions are admitted to be soft. According to NSA, the STU-III program will feature the capability for multilevel security, availability of Type 2 units to the private sector, and interoperability among all STU-III users. This will make the units attractive to a broad range of Government and private sector users.

The first production contracts were awarded in July 1986 to three vendors—AT&T, RCA, and Motorola. They are authorized to market their Type 2 product directory to the private sector. The 2-year, fixed-price contracts totaled about $190 million for 49,640 units. (See section above on Secure Voice Programs.)

NSA reports that the STU-III vendors still consider the government-contractor and other segments of the private sector market to be "embryonic, in that customers have expressed interest but are waiting to seethe product. Sample Type 2 units will be available in 1987, at which time vendors are expected to begin more active marketing efforts. According to NSA, Type 2 units could be delivered to private sector customers beginning in January 1988. The production contracts contain an add-on option allowing additional STU-IIIs (see above) to be produced at a reduced unit cost, in the $2,400 to $2,600 range. [36]

Almost all of the current order was for Type 1 units intended for classified uses, but 300 Type 2 units for unclassified, but sensitive information were also included in the initial contract. NSA will be the source of all cryptographic keys for the STU-III phones, including those purchased by private sector users. For the Type 2 phones, users will be able to establish their own internal procedures for key management, except key generation. Type 2 users within the Government will obtain their keys directly from NSA; private sector users will order keys from NSA via their STU-III vendors. [37]

The Secure Data Network System.–The Secure Data Network System (SDNS) project seeks to design an architecture for secure computer networks. The project will provide a security architecture design for networks that transmit digital data between computers. The project, certain aspects of which are currently classified, is sponsored by NSA and includes participation by NBS, the Defense Communications Agency, and about a dozen computer and communications vendors.

SDNS is intended to support both classified and unclassified applications. The system will provide confidentiality, data integrity, message authentication, and access control services. The services and standards for them are being designed to be compatible with those being developed by the International Organization for Standardization (IS0). Currently, the project is in the prototype development stage. Hardware is being developed and tested for performance, interoperability, and conformance with IS0 standards.

[34] Harold E. Daniels, NSA S-0033-87, Feb. 12, 1987, p. 4 of Enclosure 3.

[35] "STU-III Program Status," enclosure in letter from D. Latham to OTA, Nov. 7, 1986.

[36] NSA response to OTA questions on STU-III: NSA S-0033-87, Enclosure 1, Feb. 12, 1987.

[37] Ibid,

Encryption capabilities will be provided with two different NSA-supplied algorithms, both of which will remain classified. A Type 1 algorithm will be used for encrypting classified information and a Type 2 will be used for unclassified but sensitive information.

Raising Private Sector Awareness.- The Federal Communications Commission (FCC) is taking steps to alert the private sector to the vulnerabilities of communications systems. The FCC recently issued for NSA a public notice advising licensees and users that "the Nation's telecommunications systems, particularly those involving terrestrial microwave transmission media and satellites, are extremely vulnerable to unauthorized access. [38] This notice, which also applies to telecommunications services or equipment that bypass public-switched services, encourages concerned users to seek assistance from NSA in "identifying approved devices for the protection of sensitive, but unclassified, national security-related communications (Government or nongovernment). [39]

Implications of Merging Defense, Civilian Agency, and Private Sector Requirements

Advocates of combining security standards for unclassified information and guidelines for Government agencies with those for the private sector argue that aggregating markets will permit manufacturers to enjoy production economies and result in lower prices for safeguard products. Moreover, some feel that the current markets for computer and communications safeguards, particularly for trusted operating systems and cryptographic products, are "fragile. They argue that one coordinated set of Federal standards is needed to encourage and strengthen these markets. Critics of the present approach of National Security Agency (NSA) standards development and product certification see these as not fully responsive to current and evolving defense, civilian, and business needs.

There is some early evidence that NSA has already begun to encounter difficulty in satisfying the diverse needs of the private sector, beginning with the banking industry. (See ch. 6.) Moreover, NSA's controlling role may raise barriers to market entry by new vendors. At a more fundamental level, NSA's national security and signals intelligence interests in controlling encryption technology appear in tension with its new role in developing and disseminating safeguard technologies and products. (See below and ch. 7.)

Possible Barriers to Market Entry .–Only "qualified" manufacturers meeting the NSA criteria noted earlier will have access to NSA designed and endorsed standard cryptographic modules. Moreover, there will be accountability requirements for all modules and, even though the hardware modules themselves will be both unclassified and tamperproof to prevent reverse engineering, NSA may place restrictions on their export. (See below.)

The embeddable modules are being produced by the 11 large electronics firms mentioned above, NSA's "industry partners. " Because of the limited number of these firms and because they will most likely also produce host products incorporating the modules (for the Commercial Communications Security Endorsement program), some prospective entrants into the host product market have expressed concern that competition in this potentially lucrative market will be essentially limited to firms already participating in the module program. Faced with the prospect of purchasing the embeddable modules from large, vertically integrated competitors, some prospective entrants fear that NSA's tight controls on its commercial programs will limit competition.

NSA, on the other hand, does not consider the qualification criteria particularly burdensome, but, rather, reasonable. For instance, NSA notes that there are over 13,000 Defense Investigative Service cleared facilities in the United States and that cryptographic design

[38] Federal Communications Commission, Security and Privacy of Telecommunications, Public Notice 6970, Sept. 17, 1986.
[39] FCC Public Notice 6970, Sept. 17, 1986.

information is classified with access limited to U.S. entities in accordance with prudent overall security considerations. Similarly, NSA considers that decisions about the quality and market criteria will be fairly executed, with ample opportunity for vendors and potential vendors to present their cases. According to NSA, host vendor participation in the CCEP program has already exceeded participation in the DES Endorsement Program. [40]

As to competition in the host product market, NSA's stated intent is to make the Development Center for Embedded Communications Security Products (DCECP) modules competitively available to host manufacturers. All 11 of the DCECP module vendors have access to both Types 1 and 2 design documentation and, according to NSA, it is a vendor decision as to which module(s) to fabricate and produce. The Government owns the designs and NSA has stated that, should a particular module not be chosen by any of the 11 manufacturers for fabrication and production, or should there not be competitive sources for a given module, then the agency will seek additional sources for the modules. NSA also notes that, in order to achieve scale economies, competitors may sell to each other–a practice that is common in the electronics industry. [41]

DoD Control of Encryption Technology.– NSA sees its signals intelligence mission to beat risk if effective cryptography were available worldwide. As a result, NSA faces tensions between its missions of encouraging domestic use of effective encryption and other safeguards while controlling the transfer of encryption technology overseas. Thus, its strategies to improve the availability of safeguards for use by U.S. nondefense Government agencies and businesses also include controls on the dissemination of such products and technical data, some of which have already begun to cause new tensions with the private sector.

Cryptographic hardware and software are controlled by bilateral agreements and by patent and export control legislation and regulations, including the Export Administration Regulations, the Invention Secrecy Act (35 U.S.C. 181 et. seq.), and the International Traffic in Arms Regulations (ITAR), " as discussed in chapter 6. All equipment and systems based on DES, including those for automatic data processing file security and message authentication for electronic fund transfers, are included on the ITAR Munitions List and fall under the jurisdiction of the Department of State's Office of Munitions Control (OMC). OMC licensing agreements are coordinated with NSA. [43]

The exportability of cryptographic safeguards is an important consideration for many businesses that have overseas correspondents or subsidiaries. Prominent among these is the banking industry, which has spent some years developing techniques and standards for transaction authentication and confidentiality. These are based on DES, which can be licensed for export and use abroad. When NSA announced its planned replacement of DES with secret (CCEP) algorithms, bankers and the American Bankers Association (ABA) became concerned that the CCEP algorithms and modules could not be used by the financial industry as a substitute for DES. For one thing, reliance on one or a few algorithms would be unacceptable for use in some foreign countries or banks, even if NSA would permit their use abroad. Also, according to the initial NSA announcement, the (Type 2) modules may not be used internationally or placed in equipment for use by non-U. S. entities.

Finally, the bankers found the prospect of NSA retaining control of the cryptographic keys to be an unacceptable transfer of bank responsibility to a Government agency. As of mid-1987, NSA and ABA were still discuss-

[40] Harold E. Daniels, Jr., NSA S-0033-87, Feb. 12,1987, pp. 8-9 of Enclosure 2; p, 5 of Enclosure 3.

[41] Ibid., pp. X-10 of Enclosure 2.

[43] J. Multilaterally agreed upon export controls are determined through an international coordinating committee (COCOM) whose membership includes representatives of the United States and 13 L[T]. S, allies,

[44] J. Smaldone, Office of Munitions Control, personal communication with OTA staff. Sept. 24,1986.

ing whether NSA would provide an acceptable exportable module for use overseas to authenticate financial transactions. In mid-February 1987, NSA and ABA reached agreement that NSA would continue to support the financial industry's use of DES-based technology until an acceptable replacement is available.[44]

NSA appears to be reconsidering the exportability issue for Type 2 modules. In February 1987, in response to a question from OTA, NSA officials stated that:

> The NSA desires that host products employing Type 2 modules be usable by U.S. entities outside the U.S. For example, a U.S. firm operating in Europe should be able to purchase and use a Type *2* product, or a foreign subsidiary should be able to use a Type 2 product as long as ownership was maintained by a U.S. entity. Use by foreign firms or individuals, when it is in the U.S. interests for interoperability is possible, depending on the country involved and inter-country agreements. [45]

The various NSA outreach and industry partnership activities seem tailored to the agency's dual missions of encouraging the use of safeguards while controlling the spread of cryptographic and cryptanalytic expertise. For the former, NSA uses site visits, briefings, exchanges of personnel and information, and product evaluation and endorsement in addition to written standards and guidelines. For the latter, NSA makes cryptographic hardware and interface specifications generally available to host equipment vendors and users, without broadly transferring expertise in cryptographic design and cryptanalysts. For instance, it is unclear whether even the 11 module manufacturers know all the cryptologic criteria used by NSA in developing the algorithms, although NSA gives them the design information and expertise needed to manufacture the hardware that implements the algorithms.

In contrast, the DES standard as promulgated is public information, not limited to specific manufacturers and vendors, and provides more visibility into the algorithm itself. The fact that the algorithm was published made possible independent evaluations of its robustness, as well as (unvalidated) software implementations, thereby contributing to private sector capabilities in commercially useful cryptography.

On the other hand, NSA believes that assertions to the effect that current policies and the DCECP and CCEP programs limit competition and stifle private sector innovations and development are unsupported. According to NSA officials, the agency is actively encouraging private sector innovation and the development of information safeguards for business needs. For example, NSA cites the CCEP program, in which prospective host product vendors determine which products to produce based on their assessments of market needs.

Moreover, part of the rationale for NSA's approach is to use interfirm competition to drive down the cost of information security products like the STU-III phones. NSA and the rest of DoD have been concerned that relatively high costs have limited their use within DoD and elsewhere. The resulting small market was not attractive to producers. By making information security products more affordable, NSA hopes to increase their availability and use. In achieving this, according to NSA, "technological competitiveness is the goal in driving costs down versus cryptographic competitiveness which does nothing for cost and can have a deleterious effect on national security. '[46]

Technology Development and Dissemination.–After a number of DoD-sponsored studies and demonstration projects during the 1970s to address technical problems associated with controlling the flow of classified and other information in multiuser computer systems, the DoD Computer Security Initiative was

[44]Cheryl W. Helsing, Testimony on Behalf of the American Banking Association before the House Committee on Science, Space, and Technology, Feb. 26, 1987.

[45]Op. cit., Harold E. Daniels, Jr., NSA S-0033-87, p. 10 of Enclosure 2.

[46]Harold E. Daniels, Jr., NSA S-0040-87, Feb. 20, 1987, Enclosures D and E.

started in 1977. Concurrently, the National Bureau of Standards (NBS) began to define the construction, evaluation, and auditing of secure computer systems. As an outgrowth of recommendations from a 1978 NBS workshop paper on criteria for evaluating technical computer security effectiveness, and in support of the DoD Computer Security Initiative, the MITRE Corp. began to develop a set of criteria for assessing the level of trust that could be placed in a computer system to protect classified data.

In 1981, the DoD Computer Security Evaluation Center was established to continue the work started under the DoD Computer Security Initiative. The center, located within NSA, was renamed the National Computer Security Center after its responsibilities were expanded by National Security Decision Directive 145 (NSDD-145).

The National Computer Security Center (NCSC) developed the "Orange Book" criteria for evaluating multilevel security in commercial computer systems. The original criteria were published as the Department of Defense Trusted Computer System Evaluation Criteria (CSC-STD-001-83, August 15, 1983). A derivative but slightly different document was later published as DoD 5200.28-STD in December 1985. The Orange Book criteria evolved from the earlier NBS and MITRE work." NCSC has also released "Yellow Books" that help users apply the comprehensive Orange Book criteria to specific computer facilities.[47]

The criteria specify four divisions, ranging from Division D (minimal protection) up through Divisions C (discretionary protection) and B (mandatory protection), to the most comprehensive Division A (verified protection). Each division represents an improvement in the overall confidence that can be placed in the system to protect information. Within divisions C and B, security classes such as Cl, C2 or Bl, B2, and B3 correspond to progressively stronger security features.

NSA produces a number of computer security documents ranging from trusted operating systems (the "Orange" and "Yellow Books' to forthcoming criteria for trusted computer networks and data bases.[49] Some users apparently have reported difficulties in interpreting the Orange Book criteria at the higher protection levels; as one response to this, NSA has developed a rules-based expert system available to guide users through the Yellow Books.

The Orange Book criteria have been adopted as a DoD standard (DoD 5200.28 -STD, December 1985), and therefore these security requirements must be included in specifications for new systems being developed by DoD. However, the question of whether the Orange Book criteria and evaluated products program will best serve the unclassified, but sensitive information security needs of civil agencies and the private sector is being debated within the computer-security community, especially outside NSA. (See the section below on differences between military and commercial models of security.) As of May 1987, the NCSC's Evaluated Products List reported security class ratings according to the Orange Book criteria for 8 products, and about 20 more products were being evaluated.[50]

[47]From information on the history of the *Orange* Book criteria contained in DoD 5200.28 -STD, which provides a more detailed history and rationale for the trusted computer system evaluation criteria.

[48]DoD Computer Security Center: "Computer Security Requirements: Guidance for Applying the DoD Trusted Computer System Evaluation Criteria in Specific Environments (CSC-STD-003-85)," June 25, 1985; and "Technical Rationale Behind CSC-STD-003-85: Computer Security Requirements (CSC-STD-O04-85), " June 25, 1985.

[49]Presentation by P. Gallagher of NSA, at an IEEE Subcommittee on Privacy meeting at George Washington University in Washington, D. C., Nov. 13, 1986.

[50]Some information on the evaluated products program was contained in a letter from Harold E. Daniels, Jr., NSA S-O033-87, Feb. 12, 1987, p. 7 of Enclosure 2. See also: National Computer Security Center, *Evaluated* Products *List for Trusted Computer Systems*, Dec. 1, 1986 (updated May 31, 1987).

OBJECTIVES AND PROGRAMS UNRELATED TO NATIONAL SECURITY

Background

As part of this study, OTA surveyed the data and information security procedures, policies, and practices of large U.S. corporations. The survey also tried to determine the extent to which these firms are aware of Government-sponsored assistance and whether they have been affected by National Security Decision Directive 145.

The survey was self-administered at an October 1986 meeting of Palmer Associates, a group of computer audit directors of Fortune 100 companies. Questionnaires were completed by all 26 people present, a sample that is far too small to be representative of U.S. industry at large or for statistical generalizations.

Nevertheless, the results are of value for two major reasons. First, they illustrate the perceptions of some knowledgeable corporate leaders about security needs and practices. Second, the vast majority of the respondents were from nondefense companies (92 percent, with 42 percent from banking alone), while most of NSA's experience with the private sector has been with defense contractors. The survey results may shed some welcome light on the desirability and feasibility of NSA's plans to meet aggregated users' needs with one set of standards, guidelines, and technologies, and can provide a context for the section below on differences between military and commercial models of information security.

Also, the consulting firm of Ernst & Whinney included some of the same questions in a separate survey that was self-administered by attendees of the Computer Security Institute's 13th Annual Conference held in November 1986 in Atlanta, Georgia. A total of 562 completed questionnaires (a 12 percent response rate) were returned on site or by mail; 141 responses (25 percent) were from Government employees and the remainder came from a broad spectrum of business and industry. Of the respondents, another 18 percent were from manufacturing, 15 percent from financial services, 9 percent from insurance, and 8 percent from communications firms. Only 3 percent of the respondents identified themselves as from the defense industry. With Ernst & Whinney's permission, some of their survey data are used in this chapter, in addition to the OTA survey data.

Private Sector Motivations

Private industry and civilian agencies want information safeguards to:

- protect corporate proprietary or sensitive information from unauthorized disclosure or access and ensure the integrity of data and its processing;
- reduce losses from fraud and errors in electronic funds transfers and other financial transactions, limit associated increases in insurance premiums, and limit exposure to legal liabilities for preventable losses; and
- take advantage of new opportunities to reduce costs.

Box E provides several indicators of increased private sector interest in electronic safeguards.

Protection of valuable corporate electronic information from disclosure (confidentiality) is important to many firms, but this need is not necessarily a firm's major concern for information security. The OTA survey found that the 26 respondents placed roughly equal importance on integrity, confidentiality, and

Box E.—Indicators of Private Sector Interest in Safeguards

Even though many industry spokesmen consider the market for many advanced safeguards fragile and emerging, OTA has noted a number of indications of growing private sector interest in improved safeguards, including:

- *Rapid growth in the number of computer-communications security conferences during recent years and in their attendance* levels.—Attendance at the National Computer Security Conference, sponsored jointly by the National Security Agency (NSA) and the National Bureau of Standards (NBS), increased three-fold in the last 7 years, from about 350 in 1980 to more than 1,000 in 1986. Capacity constraints at NBS conference locations have forced sponsors to limit attendance. Some other conferences, such as the Institute of Electrical and Electronics Engineers (IEEE) Symposium on Security and Privacy are also limited by space constraints. Attendance at the Computer Securit y Institute's annual Computer Security Conference/Exhibition doubled–from 600 to l,200–between 1981 and 1985, and the American Society for Industrial Security Seminar and Exhibition has expanded to include computer security, biometrics, and access control. In addition, many new conferences and workshops given by security consultants and user groups have sprung up over the past 3 years. Among the latter are conferences and workshops for users of the Top Secret and RACF access control software packages. Other annual conferences include CRYPTO in the United States and EUROCRYPT, both sponsored by the International Association of Cryptologic Research.
- *Increases in the level of sales of safeguard equipment and* software. -According to market reports, installations of two of the most popular commercial access control software packages, ACF2 and Top Secret, have grown by more than a factor of 10 over the past 6 or so years.
- *The* rise *in the number of computer and communications security consultants and in the number of organizations for security professionals.-The* number of security consultants listed in directories have increased, and new professional groups are forming, such as the Information Systems Security Association (ISSA). Consulting firms are expanding their information security practices and new services organizations are being established. such as the International Information Integrity Institute (SRI International).
- *The increasing number of technical articles being published on topics related to computer and communications security .—OTA* staff did a word search using the abstracts of articles published in the ABI/INFORM journal set, a collection of more than 650 U.S. and foreign business publications including such areas as accounting, banking, data processing, economics, finance, insurance, and telecommunications. The 200-word abstracts for the years 1971, 1976, 1981, and 1985 were searched for 5 selected phrases (computer security, communications security, encryption, data integrity, and personal identification) in order to determine whether the relative frequencies of these had increased. OTA found that the number of abstracts including these phrases had grown in real as well as nominal terms, in particular, the phrase "computer security" occurred in only one out of 1,737 abstracts in 1971, but occurred in 268 out of 38,375 in 1985—a 10-fold increase in relative frequency (none of the other 4 phrases occurred in any of the 1,737 abstracts in 1971). The phrases "data integrity" and "encryption" occurred in only two and eight out of 14,356 abstracts, respectively, in 1976. By 1985, they occurred in 45 and 85 out of 38,375 abstracts, respectively–a three-fold and ten-fold increase in relative frequency. The phrases "personal identification" and "communications security" occurred infrequently and did not show significant increases in relative frequency.

reliability/continuity of service as components of their organization's information security, with integrity being rated slightly more important overall. The larger Ernst & Whinney survey found similar results, with both Government and nongovernment respondents rating integrity slightly higher than confidentiality and reliability/continuity. Interestingly, Government respondents rated confidentiality slightly higher than continuity of service, while the opposite was the case for nongovernment respondents.

Encryption or access control technologies can protect valuable proprietary information from disclosure, but they can also preserve its integrity and protect it from accidental or malicious modifications or deletions. This can be particularly important where large databases are a major revenue-producing asset. The regional Bell operating companies, for example, safeguard their on-line database for their *Yellow Pages* to preserve the integrity of the data and to prevent unauthorized use, not to prevent disclosure. In that sense, a recent news story reported that a disgruntled employee had attempted to rewrite parts of the 1988 edition of the *Encyclopedia Britannica.* The sabotage attempt failed, according to a company spokesman, because of safeguards that prevented unauthorized changes to the computer database.[51]

Most of the OTA survey respondents and almost 90 percent of the Ernst& Whinney survey respondents judged information security as being of 'fair' or 'extreme' importance to their organizations. Of the Ernst & Whinney respondents, Government respondents assigned slightly more importance overall to information security than did the nongovernment respondents.

All the OTA survey respondents noted an increase in the importance of data and information security to their firms over the past 2 years. About one-third reported "significant information or data security problems" during the past 2 years, mostly in the form of unauthorized access and loss of integrity (in one case, engineering data was destroyed). In only one instance was loss of confidentiality cited, resulting in invalid competitive bids—which may be an indication of the difficulty of detecting some misuses, rather than their absence. Only 2 percent of the information handled by these firms is classified for reasons of national security, according to respondents to the OTA survey.

The majority of Ernst & Whinney survey respondents considered that the security risks faced by their organizations have increased over the past 5 years, and about one-third of the business and one-fourth of the government respondents considered that these risks were not adequately met. Half of the respondents reported financial losses as a result of security problems or downtime, mostly under $50,000, although a few losses were reported to be in excess of $1 million (note that this question included losses due to downtime, which the OTA survey did not include). About one-third of the respondents reported non-financial losses, mostly in the form of unauthorized access by employees and hackers. For Government respondents, about 31 percent of the information mix handled by their organizations was classified for purposes of national security, versus only 4 percent for nongovernment respondents.

Reducing EFT Fraud and Other Losses.—U.S. banks transferred some $167 trillion in 60 million separate transactions in 1984. The actual amount of wire transfer fraud experienced by banks is unknown. One estimate by the Bureau of Justice Statistics suggests aggregated electronic fund transfers (EFT) and automated teller machine (ATM) losses of $70 million to $100 million a year during the early 1980s, but a large fraction of this figure is due to ATM losses from fraud (by "con men, " etc.) against the owners of the bank cards. Another Bureau

[51] "Britannica Sabotage Thwarted, " Washington *Post*, Sept. 6, 1986, p. D3.

of Justice Statistics report examined some 139 problem wire transfers. It found an average potential loss per transaction of $800,000, although some potential losses were significantly larger."

Similarly, an American Bar Association (ABA) survey of private and public sector organizations found that one-quarter (72) of those responding reported "known and verifiable losses due to computer crime in the last 12 months. Losses reported by respondents overall ranged from a few thousand dollars to more than $100 million. Most losses reported by the (anonymous) respondents were less than **$100,000.[54]"**

A large survey by the American Institute of Certified Public Accountants revealed that 2 percent (105) and 3 percent (40), respectively, of the banks and insurance companies surveyed had experienced at least 1 case of fraud related to electronic data processing (EDP). Most perpetrators were employees. More than 80 percent of the frauds involved amounts under $100,000."

The Department of Justice Bureau of Justice Statistics (BJS) recently examined the scope of EFT fraud, based on extrapolations from a limited sample of 16 banks. The BJS study suggested annual losses nationwide in the $70-$100 million range for automatic teller machine fraud. Twelve of the banks reported 139 wire transfer fraud incidents within the preceding five years, with an average exposure to loss (before recovery efforts) of some $880,000 per loss and an average net loss (after recovery efforts) of about $19,000 per incident.[55]

Whatever the actual amount of the losses, there is another indirect indicator that this is a serious problem: insurance premiums are rising for protection against fraud and other types of losses related to electronic transfers of funds.[56] During the past year, financial institutions' motivations to safeguard value-bearing transactions-EFTs, letters of credit, and securities transfers-have been strengthened by actions of their insurers, some of which are raising premiums and/or requiring the use of message authentication methods approved by the American National Standards Institute (ANSI). As industry applies safeguards more widely and as the use of certified safeguards becomes more commonplace, expectations for responsible corporate behavior will be raised. A new standard, and perhaps a legal criterion, appears to be evolving for gauging responsible corporate behavior, or "due care, in businesses where firms are expected to provide reasonable safeguards for information whose loss could do significant harm.

The wholesale banking industry is leading this trend, prompted by liability and "due care' considerations, by the recommendations of internal and external auditors, and by Treasury Department policies. Treasury has issued policy directives requiring all Federal electronic fund transactions to be authenticated by June 1988. Dated August 16,1984, TD-81.80

[52]See U.S. Congress, Office of Technology Assessment, "Ch. 5, Computer Crime, " *Federal Government Information Technology: Management, Security, and Oversight, OTA-C IT-297* (Washington, DC: U.S. Government Printing Office, February 1986), for an overview of the scope of computer-related crime and losses from electronic fund transfers and automated data processing.

[53]Report on Computer Crime, Task Force on Computer Crime, Section on Criminal Justice, ABA, 1984.

[54]American Institute of Certified Public Accountants, EDP Fraud Review Task Force, *Report on the Study of EDP-Related Fraud in the Banking and Insurance Industries, 1984.*

[55]Bureau of Justice Statistics Report NCJ-1OO461, *Electronic Fund Transfer Systems Fraud,* April 1986.

[56]The experience of a west coast bank illustrates the magnitude of the changes in coverage being offered by insurers for EFT loss claims. Until recently, the bank's insurance coverage cost about $1 million annually, and provided protection of up to $50 million per electronic transfer claim, with a $1 million deductible. The policy premium in mid-1 986 rose to $5 million, with a $10 million deductible, and an upper limit of $100 million for total annual claims. *[Source:* OTA staff discussion with bank officials, May 1986.]

specified that Federal EFT transactions be authenticated using measures based on DES and conforming to ANSI standards. This action is expected to have widespread effects throughout the banking industry because of the large number of systems and communications links that will use the system, and because some standards set by Treasury and the Federal Reserve System (which serves as the interface between Treasury and the wholesale banks) become defacto industry standards. As certified hardware for authentication becomes more widely used, economies of scale will lower prices for authentication hardware. As prices fall, additional end users are likely to adopt techniques and hardware to safeguard other business functions, creating a ripple effect throughout the private sector.

Thus, an early and important exception to the non-recertification of DES was made by NSA in the area of electronic fund transfers. Through a memorandum of understanding, the Treasury Department will certify commercial data security devices for securing fund transfers, with technical guidance and support from NSA and NBS. DES will remain the encryption algorithm for EFT transactions while authentication measures will be specified by ANSI standards adopted by the wholesale banking community." More recently, NSA agreed to support use of the DES for bank message authentication until an acceptable replacement became available. Widespread use of DES to authenticate electronic fund transfers will increase demand for DES-based hardware. That could lower its price and encourage its adoption for other applications in wholesale and retail banking and elsewhere. As an example of a retail banking application, the DES is used to encrypt customers' personal identification numbers in interbank automatic teller machine networks in the United States and Canada.[58]

A superseding Treasury Directive, TD-16.02 (dated October 2, 1986), extended the authentication requirement to securities transfers and stated that equipment designed and used to authenticate Federal EFTs must comply with Federal Standard 1027, which specifies security requirements to be satisfied in implementing DES (FIPS Pub. 46). Keying material used in DES authentication must be generated and processed in accordance with ANSI Standard X9.9. The broader requirement is expected to speed the dissemination of authentication techniques throughout the private sector.

A number of private financial institutions are taking aggressive steps to prevent certain types of misuse. Citibank, for instance, now has more than 4,000 encrypted links overseas. Similarly, the private Clearing House Interbank Payments System (CHIPS), whose $240 billion in daily settlements is second in size only to the Federal Reserve System, uses ANSI-approved standards to authenticate its transactions.[59] Large U.S. banks have also been among the most active participants in the development of technical standards through ANSI (see below).

Reducing Costs.—Companies can also reduce the costs of routine business transactions by conducting them via computer-to-computer communications that make use of cryptographic-based authentication techniques. These inter-organization transactions use standardized formats for the electronic interchange of business data between independently organized, owned, and/or operated computer and communication systems. This is accomplished by each corporate participant assembling its transaction data in predefined sequences, called "transaction sets. "

[57] Memorandum of Understanding #S52-99-84-018, Parts IV and V. This memorandum may be renewed in 1987, according to NBS staff.

[58] Eddie Zeitler, Security Pacific National Bank and Nancy Floyd, Citicorp/Quadstar. Personal communications with OTA staff, Feb. 18, 1987.

[59] Authentication in CHIPS, New York Clearing House, Jan. 17, 1985.

In 1986, CHIPS transactions amounted to $125 trillion, compared with $124.4 trillion in domestic transactions handled by the FEDWIRE system. The FEDWIRE system handles a greater volume of transactions than CHIPS, and has many more on-line correspondents (7000 depository institutions compared to the 121 CHIPS member banks). [Source: Florence Young, Division of Federal Bank Operations, Federal Reserve System. Personal communication with OTA staff, Feb. 13, 1987.]

Several industry-specific interchange standards have previously been developed, including transaction sets for air, motor, ocean, and rail transportation, as well as for public warehousing, and for the grocery industry. Development of an American National Standard for electronic data interchange is under way, intended to replace the many paper and special-purpose business methods by 1988. One of the long-term goals of this standard is the realization of paperless trade transactions and transportation arrangements. Standards for this purpose are being developed by the ANSI X12 Committee, which was chartered in 1978. The first set of X12 standards for electronic business data interchange was approved by ANSI in 1983, and more were published in 1986.

The national standards are intended to be broad enough to encompass all forms of business transactions amenable to standardization, including inter-industry transactions. The electronic transactions, referred to as Electronic Data Interchange (ED I) or Electronic Business Data Interchange (EBDI), are intended to reduce business costs by speeding up the purchase order cycle, reducing the inventory buffers firms must carry, and streamlining cash flow. Dozens of common transactions will be integrated using these standards, including purchase orders, invoices, shipping notices, check payment vouchers, requests for quotations, and marketing information.[60] These transactions amount to billions of dollars annually. An estimated $38 million worth of them were handled electronically in 1985; by 1990, electronic business transactions are expected to amount to more than $1 billion.[61]

These standards, or some compatible form of them, may also be adopted worldwide, thereby facilitating international transactions in different currencies. For this reason, any message authentication product, such as that required for business data interchange will have to be eligible for use in other countries. The current ANSI authentication standard, based on the DES, is exportable, but its replacement may not be.

The original focus area for electronic data interchange was in transportation, beginning in 1968.[62] The Transportation Data Coordinating Committee (TDCC) worked with representatives of the rail, motor, ocean, and air transport industries to develop EDI transaction sets for these modes. The first successful data interchange transmission occurred with railway bills, in 1975. Around the same time, TDCC organized a group of computer and communications experts to develop specific business applications of this type of electronic transaction. Among the outcomes of this group activity were the development of purchase order and invoice transaction sets and movement toward generic transaction sets for industry. In the early 1970s, large corporations, such as Sears, JC Penney, and K-Mart had started transmitting purchase orders electronically, with specialized formats. This was feasible in part because these retailers were often their suppliers' sole or largest customer. However, benefits due to improved transaction accuracy and timeliness accrued to both parties, increasing interest in electronic transactions.

Movement toward further development of generic transaction sets was formalized in 1978, when the ANSI X12 Committee was formed. TDCC and the Credit Research Foundation provided technical support to the new committee, and TDCC is the current X12 Secretariat. In 1979, the grocery industry began its industry-specific Uniform Communication Standard (UCS), which is compatible with the EDI architecture developed by TDCC for the transportation standards. Subsequently, standards for public warehousing applications (Warehouse Information Network Standards,

[60]See: Jack Shaw, "Electronic Business Data Interchange: A New Strategy for Transacting Business," *MSA Update, Management Science America, Inc.*, March' April 1985; "Detroit Tries to Level a Mountain of Paperwork, *Business Week*, Aug. 26, 1985, pp. 94-96.

[61]"Management Information Systems Week, Jan. 20, 1986. Estimates provided by Jack Shaw at the ANSI ASC X12 meeting on June 9, 1986 are over $3 billion by 1990.

[62]Information on the evolution of electronic data interchange standards was provided by Paul Lemme, Transportation Data Coordinating Committee, ANSI X12 Secretariat. Personal communication with OTA staff. December 1987.

or WINS) were developed, also compatible with the EDI architecture. These standards include various security features.

The ANSI X12 Committee is developing generic standards for electronic business data interchange. In November 1986, industry representatives agreed on a common data dictionary for the ANSI X12 standards, the WINS and UCS standards, and the TDCC ED I standard.[cs] The ANSI X12 Security Structures Taskgroup is developing transaction security standards under the auspices of the X12 Finance Project Team, and the X 12 Committee has joined with the ANSI X9 Committee to deal with encryption and encryption-related business requirements. According to the X12 Secretariat, the latter include: electronic signatures ("telex signature"); data integrity, "hash controls" (digests); message authentication and sender verification; confidentiality of business data error detection; end-to-end security; and protection against replay, spoofing, modification, or impersonation.

Benefits from electronic transactions are expected to be substantial for diverse user groups, and some are already being realized. In 1980, a report prepared for the American Grocery Industry projected $300 million in profits for the industry as a result of implementing standardized electronic transactions. The grocers' UCS standards were completed in 1981, and the resulting industry gains have reportedly exceeded the projections.[c4] The Automotive Industry Action Group, composed of the the major U.S. automobile manufacturers and about 300 of their largest suppliers, began their movement toward standardization of electronic business transactions in 1981. According to some estimates, General Motors and Ford expect to realize a $200-per-car savings, or some $1 billion a year, on a typical production volume of 5 million cars per year, through use of electronic business data interchange.[c'] Caterpillar Tractor Co. has instituted an electronic transaction system linking some 400 sites.[cc]

Because of the automobile industry's large number of suppliers, contractors, and distributors, their use of the new data interchange standards is expected to accelerate the spread of these standards to other industries. These include metals, plastics, and rubber, as well as chemicals, transportation, electronics, aerospace, banking, and retail sales.[c7] The movement toward electronic business transactions is giving rise to new, network-based "electronic clearinghouses' with market entrants such as IBM, GTE Telenet, GEISCO, Tymshare, and GM's Electronic Data Systems.[68]

Potential savings to the Federal Government from electronic purchasing alone have been estimated to be $20 billion/year or more.[69] The DoD, for instance, has begun to use electronic data interchange to reduce the time required to get supplies to overseas commissaries, and expects to shorten immediately the 75-day purchase cycle by 5 or 6 days, thereby reducing inventory requirements. Other commissary and procurement paperwork-reduction projects have been under way within DoD for a few years.[70]

[63]Elisabeth Horwitt, "Move to EDI Gathers Steam as Standards Clear, Benefits Grow," *ComputerWorld*, Dec. 15, 1986, p. 5.

"Paul Lemme, TDCC. Personal communication with OTA staff, December 1986.

[65]Ford's estimate is from "GEISCO Plans To Move Rockville Jobs in Bid to Get Edge in Global Markets," *Washington Post*, Sept. 29, 1986, Business Section, p. 4. The cost savings for GM is from a presentation by Jack Shaw at the ANSI X12 ASC meeting, June 9, 1986. This estimate does not include other potential savings from ED I facilitating just-in-time manufacturing with reduced supply inventories. Shaw also reported that implementation of EDI enabled one large Eastern railroad to halve its purchasing data processing staff and is expected to cut another railroad's purchase order lead time from 10 days to 3.

[66]Irwin Greenstein, "Caterpillar Erects Paperless Network," *MIS Week*, Jan. 20, 1986.

[67]*Business Week*, op. cit., Aug. 26, 1985.

[P'] GEISCO Plans . . . .," *Washington Post*, op. cit., Sept. 29, 1986.

[69]Jack Shaw, ANSI X12 meeting on June 9, 1986.

[70]Brad Bass, "Moving Data Electronically Expedites Supply Delivery," *Government Computer News*, Jan. 30, 1987, p. 22.

Linkages in and Contrasts Between Defense-Intelligence and Other Needs

Some Linkages Between Private Sector Activities and Federal Policy .—Private industry and civilian Government agencies' interest in safeguarding their computer and communications information are becoming intertwined with Government policies even though these interests are increasingly independent of national security. The linkages between private users and the Government, and between the civil agencies and NSA, tend to blur this independence. These linkages are especially influential where NSA's technical expertise or Government certification is important, or where Government agencies, as major purchasers, tend to drive commercial equipment designs.

Although NSA's technical knowledge in high quality cryptography and cryptanalysts is acknowledged to be the cornerstone of U.S. capabilities, very little of it is unclassified. Because of this, private users depend on NSA's willingness to provide information and advice, which currently takes place, in part, in the form of NSA-certified commercial products.

Understandably, private sector users place a high value on certified, validated, and standardized safeguard products. This dependence has required considerable involvement by NBS and NSA in the absence of private sector institutions fully competent to independently develop standards and certification processes. However, NSA's plans to replace DES in 1988 with hardware modules that use secret algorithms will tend to deepen and perpetuate private sector users' dependency on NSA expertise as long as these users have no independent alternative for developing a certified, nonsecret, and exportable successor to DES.

Government agencies represent a large market for some information security products, therefore their choice of standards has a significant influence on manufacturers. According to estimates from a study conducted by the Electronic Industries Association (E IA) in cooperation with NSA, Federal and private sector budgets for information security totaled some $3 billion, split evenly between communications security and computer security. [71]

Other important linkages between Government policies and the private sector, and between defense and civilian agencies, are in the areas of security awareness, education, and assistance. During the past few years, there has been mounting confusion concerning the distinction between the roles of NBS and NSA in these areas. In addition to its Federal standards development, NBS, under its authority in the Brooks Act, as amended, participates in the voluntary activities of standards organizations and works with the private sector and civilian agencies to develop computer and computer network safeguards techniques, including security components for the open system interconnection (0SI) architecture. However, NSA, under the auspices of NSDD-145, has expanded its relationships with civil agencies, providing threat assessments and awareness briefings and advice in selecting cost-effective and appropriate safeguards. NSA reports that it has provided assistance to 36 different civil agencies and departments, plus the U.S. Senate, for diverse application areas including trade and finance, drug interdiction, law enforcement, health, agriculture, immigration, and aviation and national security, [72] as well as to Government contractors and other firms. [73]

[71] Of the $1.5 billion budgeted for communications security in 1986, 66 percent was budgeted by DoD, about 7 percent by other Federal agencies, and 27 percent by the private sector (including defense firms). Of the $1.5 billion for computer security, however, DoD and other Federal agencies only accounted for 13 and 11 percent, respectively, while the private sector accounted for about 75 percent. Electronic Industries Association: "COMSEC and COMPUSEC Market Study, " Jan. 14, 1987.

[72] Agencies and departments that have been assisted by NSA include the United States Trade Representative, International Trade Administration, Securities and Exchange Commission. Federal Reserve Board, Department of Labor, National Narcotics Border Interdiction System, Immigration and Naturalization Service, Drug Enforcement Administration, Center for Disease Control, National Institutes of Health, Department of Agriculture, and Federal Aviation Administration. Harold E. Daniels, Jr.. NSA S-0040-87, Feb. 20, 1987. Attachment 2 to Enclosure D.

[73] Ibid., Attachment 1 to Enclosure D.

Vendors of safeguard technologies and private-sector defense contractors are also closely linked to Federal information security policies and programs, such as NSDD-145. Because the new, NSA-certified encryption modules are expected to have a large, stable market among Federal agencies, vendors are unlikely to attempt development of riskier, uncertified, encryption-based safeguards. Private sector users, therefore, may be faced with limited new options if the supply of encryption-based safeguards is determined by "technology push" (from NSA) rather than "demand pull" (from unconstrained market forces).

Emerging Differences.–What is open to question is the extent to which the concerns, priorities, and needs of the defense- and national security-oriented user communities are generalizable to civilian agencies and the bulk of the private sector.

One interesting set of findings from the OTA and Ernst & Whinney surveys,[7J] mentioned earlier, is based on the respondents' perceptions of who their organizations' adversaries are and illustrates an important difference between perceived Government and private sector information security needs: who the most significant adversaries are, and what level of resources they possess. Table 7 summarizes responses to a question in each survey that asked respondents to rank categories of adversaries according to how relatively important it is to protect their organizations' significant (unclassified) "company confidential" or proprietary information from them. For example, the group of 26 nongovernment individuals surveyed for OTA, predominantly nondefense Fortune 100 executives, rated foreign governments as their least important adversary. [7s]

Similarly, the larger sample of non-Government respondents surveyed by Ernst & Whinney ranked foreign government adversaries lowest overall. Instead, both non-Gov-

Table 7.—Overall Ranking of Importance as an Adversary (Highest = 7)

Category of adversary	OTA survey responses[a] Mean ranking of category	Fraction of responses ranking category #l or #2
Your competition	6.7	920/,
Some of your internal employees	4.8	31
Foreign governments	3,1	4
Your suppliers	4.1	15
Your customers	4.9	27
Public interest groups	4.0	19

aA(l respondents were non. government

Category of adversary	Ernst & Whinney survey non-government responses Mean ranking of category	Fraction of responses ranking category #1 or #2
Your competition	6.5	89%,
Some of your internal employees	4.9	43
Foreign governments	3.9	30
Your suppliers	4,1	11
Your customers.	4.7	35
Public interest groups	3.9	15

[b]Between 200-300 out of a total of 421 non-government respondents ranked each category of adversary, the rest did not rank that category

Category of adversary	Ernst & Whinney survey Government responses Mean ranking of category	Fraction of responses ranking category #l or #2
Your competition	4.1	35 "/0
Some of your internal employees	5,3	53
Foreign governments	6.1	74
Your suppliers	4,3	24
Your customers	4.5	34
Public interest groups	5.0	48

[c]Between 26-49 out of a total of 141 government respondents ranked each category of adversary the remainder did not rank that category

[74]The OTA computer security survey was conducted in October 1986, at a meeting of Palmer Associates. The 26 respondents to the questionnaire were data processing audit vice-presidents and data processing audit directors of Fortune 500 companies. Ernst & Whinney, "OTA Computer Security Survey, " OTA contractor report, Nov. 7, 1986.

Ernst & Whinney conducted a separate survey in November 1986 at the 13th annual conference of the Computer Security Institute. About 500 attendees responded to this self-administered survey, most of whom had responsibility for computer security functions. The data were made available to OTA in February 1987.

[75] One of the OTA survey respondents noted that his firm was most concerned with protecting information from foreign governments; another was concerned with protecting confidential customer information from the U.S. Government.

ernment groups considered their competition as the most important single adversary, followed by customers and some internal employees, and then by suppliers, public interest groups, and foreign governments. The Government respondents surveyed by Ernst& Whinney considered foreign governments (perhaps analogous to "your competition' for businesses) to be the most important adversary, followed by some internal employees, public interest groups, and the other categories. An important difference between business competitors and foreign government adversaries is, obviously, the level of resources that each type could deploy to gain access to information.

The Electronic Industries Association market study mentioned earlier also found "widely different perceptions of the threat to information systems and this results in different and often conflicting and competing security requirements . . ." The study notes a national security perspective that focuses on external threats while others' perceptions are of internal sources as the principal threat.[76] It also notes that businesses and civilian agencies attached considerable importance to the cost of safeguards and their effect on operations.

Other differences (and similarities) between current Government and private sector information security priorities are suggested by a survey question asking respondents to list their organizations' "top-priority" computer-security and information-security concerns. These responses are summarized in table 8. Although the same types of concerns are mentioned by Government and private sector respondents, their relative priorities are different.

An important effect of these perceptions and priorities is on the users' decisions concerning the use and choice of safeguards.

Another interesting finding from both the OTA and Ernst & Whinney surveys was the relatively low level of perceived impact (as of Fall 1986) from NSDD-145 on non-Government organizations safeguarding of unclassified information. Table 9 summarizes responses to a survey question about the impacts of NSDD-145. Almost three-quarters of the respondents (all non-Government) to the OTA survey and almost half of the non-Government Ernst & Whinney survey respondents felt that NSDD-145 had had no impact on their organizations' safeguarding of unclassified information. Moreover, fewer than 10 percent of the respondents to the OTA survey and fewer than 30 percent of the non-Government respondents to the Ernst& Whinney survey considered that the directive had impacted their firms' security practices for unclassified information "somewhat" or "greatly. [77] By contrast, the Government respondents in the Ernst a Whinney survey reported much higher levels of impact overall, with only one-quarter reporting no impact from NSDD-145 on unclassified information security and almost 60 percent reporting that the directive had impacted their organizations' unclassified information security at least somewhat.

More than two-thirds of both the OTA survey respondents and the non-Government respondents to the Ernst & Whinney survey felt that their firms' information and data security measures were at least fairly adequate to meet their needs. What is somewhat surprising is the relatively low percentages of these firms' total information and computer security expertise attributed to Government-sponsored assistance programs, conferences, and training programs. Only 2 of the 26 OTA survey respondents indicated that even a small percentage of their firms' information and data security expertise came directly from Government assistance programs. This low percentage is likely due to the composition of the Palmer Associates group surveyed and is in marked contrast to what one might expect

[70] Electronic Industries Association, "COMSEC AND COMPUSEC Market Study, '(Jan. 14, 1987. This study was based on 75 interviews, 64 of which were with Federal agencies, including 39 having defense and intelligence missions.

[77] Two firms in the OTA survey indicated that they had implemented encryption or scrambling to protect sensitive communications in response to N SD II- 145, and one of these firms also implemented access control soft ware, passwords, and acquired special communications channels.

Table 8.—Top-Priority Computer and Information Security Concerns Mentioned by Respondents

OTA survey group (non-government)	Ernst & Whinney non-government group	Ernst & Whinney Government group
Data security/data integrity	Network security	Contingency planning/disaster recovery
Network security	Data/information classification and security	Data/information classification and security
Contingency planning; training	Micro/PC security	Network security
Quality security throughout firm; telecommunications links; internal hacking	Dial-up security/communications	Micro/PC security

SOURCE Data from surveys conducted by Ernst & Whlnney In October and November 1986

Table 9.–Perceived Impacts From NSDD-145 (Fall 1986)

Question: "On September 17, 1984, President Reagan signed National Security Decision Directive 145 (N SDD-145), the National Policy on Telecommunications and Automated information Systems Security. This policy has led to much more active involvement by the National Security Agency and the National Computer Security Center in providing advice to business and industry. How has NSDD-145 impacted your organization in safeguarding information that is not classified for purposes of national security?"

	Survey responses			
Response	OTA survey total responses to question (all non-government) (23)	Ernst & Whinney total responses to question (486)	Ernst & Whinney non-government responses (364)	Ernst & Whinney government responses (122)
Not at all	74 "/0	41 "/0	46%	25%
Very little . . .	17	25	27	18
Somewhat . . .	9	24	21	33
Greatly.	0	11	6	24

SOURCE Data from surveys conducted by Ernst & Whinney In October and November 1986

from an alternative group composed of defense contractors, computer firms, or firms producing security products for the Government market. In fact, only two of the respondents to the OTA survey indicated awareness of any specific Government-sponsored information and assistance programs. Of the 22 individuals responding to a question concerning their perceptions of the helpfulness of Government guidelines, 17 answered "not at all, " while 5 said these had been "somewhat" helpful to their organizations. The respondents who did find Government guidelines helpful cited the NBS Federal Information Processing Standards (FIPS), including DES, as well as guidelines for protecting privacy-related and classified information.

Differences Between Military and Civilian Computer Security Models.–The debate about how well the NSA's Orange Book computer security standards and evaluated products program will serve the needs of civilian agencies and private businesses is receiving increased attention within the computer security community. One of the most crucial aspects of the debate concerns the security policy underlying the Orange Book criteria, the mechanisms needed to enforce security policy, and how well these match the security policies (and associated mechanisms) that are common in commercial practice. According to computer security experts at NSA, for example, the National Computer Security Center (NCSC) has worked —and continues to work— "hand in glove" with the civilian agencies to understand their needs and provide appropriate computer security solutions[7g] and, moreover, products that have been evaluated by NSA and that have received

[78]Harold E. Daniels, Jr., NSA S-0033-87, Feb. 12, 1987, p. 7 of Enclosure 2.

B- and C-level ratings are being used in the private sector (some of these, such as RACF, ACF2, and Top Secret, were developed well before the Orange Book was published but have been modified to meet Orange Book standards). Other experts disagree with this position, and argue that the security policy and mechanisms specified in the Orange Book do not meet important needs in commercial data processing.

Among the latter group are David D. Clark (MIT Laboratory for Computer Science) and David R. Wilson (Ernst & Whinney). In their paper, "A Comparison of Commercial and Military Computer Security Policies, '[79] they present a security model based on commercial data processing practices and compare the mechanisms needed to enforce this model's rules with those needed to enforce the (lattice) model of security embodied in the NSA criteria. Other experts have also offered criticisms of the Orange Book's applicability to business needs. However, a brief summary of the Clark and Wilson paper, offered here as an example, points out some of the main points of criticism.

According to Clark and Wilson, the "military" (NSA/DoD) security policy is really a set of policies designed to control classified information from unauthorized disclosure or declassification. Mechanisms used to enforce this security policy include mandatory labeling of documents or data items, assigning of user access categories based on security clearances, generating audit information, etc. The higher-level security policies include mandatory checks on all read and write transactions; these mandatory controls constrain the user so that any action taken is consistent with the security policy. In addition to these mandatory controls, discretionary controls can be used to further restrict data accessibility (e.g., "need to know" controls), but, say Clark and Wilson, these cannot increase the scope of security controls in a manner inconsistent with the underlying multi-level classification concept.

[79]David D. Clark and David R. Wilson, "Commercial Security Policies, " *Proceedings, 1987 IEEE Symposium on Security and Privacy*, Oakland, CA, Apr. 27-29, 1987.

By contrast, Clark and Wilson assert that what underlies commercial data processing security practices is the prevention of fraud and error and, therefore, that a "commercial" security policy should address integrity rather than disclosure. Some of the mechanisms to enforce this type of policy are common with those for the military model (for example, user authentication), while others are very different. Among these others, Clark and Wilson identify two principal mechanisms: the well-formed transaction (in which a user can manipulate or record data in constrained ways that preserve or ensure the integrity of the data–analogous to a paper-and-ink accounts book in which correction entries, rather than erasures, are made); and separation of duty among employees (in which the user permitted to create or certify a well-formed transaction may not be permitted to execute it—analogous to double-entry bookkeeping in which a check for payment must be balanced against a matching entry in the accounts-payable column). Separation of duty is a fundamental principle of commercial data integrity control, and is considered effective except in the case of collusion among employees.

In their paper, Clark and Wilson conclude that the integrity mechanisms inherent in the commercial security model differ from the mandatory controls in the military (nondisclosure) security model in important ways, and controls based on the military model are not sufficient to enforce the commercial (integrity) model. They then introduce a more formal model for data integrity in computer systems, based on the use of constrained data items and transformation procedures for enforcing an integrity policy. Comparing this model with other integrity models, Clark and Wilson argue that their model, unlike the Orange Book standard, is applicable to a wide range of integrity policies.

By early 1987, debate on the general applicability of the Orange Book criteria and development of alternative models of computer and information security had developed to the extent that plans were made for an invitational Workshop on Integrity Policy for Computer

Information Systems, organized by Ernst & Whinney and cosponsored by the Institute for Electrical and Electronic Engineers, the Association for Computing Machinery, NBS, and NSA's National Computer Security Center (NCSC), to address military versus commercial security policy issues. The workshop is scheduled to be held in late 1987. [80]

Civilian Agency Actions.–In addition to the NBS activities described earlier, related to DES, FIPS publications, and voluntary standards development, there are other civilian agency activities related to safeguarding electronic information. (An earlier OTA report surveys civilian agency programs for computer security.)81 The Treasury Department, for example, requires the use of safeguards for information systems that handle sensitive, as well as classified, information.[82] All Federal electronic fund and securities transfer systems must also have safeguards in place by June 1988. The requirement applies to all Federal agencies (except DoD, which has its own policy) and to wholesale banks that do business with Treasury and use the Federal Reserve System as the interface.[83] The Treasury Department Order (TO 106-09) requires that authentication measures conform to the American National Standard Institute (ANSI) X9.9 standard "or equivalent authentication technique. "8[4] According to Department of Treasury officials, the DES "is and will remain fundamental to the Department's security strategy for the foreseeable future. "[85] Treasury has announced that technology to secure Federal electronic fund transfers (EFTs) must be compatible with systems used by the Federal Reserve System and the commercial banking community. Specifically:

- Treasury will continue to support and implement ANSI financial standards as the common method for securing Federal EFTs and will only transition from the current (DES based) ANSI standards to any new ANSI standard (not based on DES) if the transition is based on "sound business decisions and security needs. "
- Treasury will rely on NSA's commitment, of November 12, 1985, that DES will be supported indefinitely for the financial community.
- Treasury will rely on NBS to continue to validate DES chips.
- Treasury will continue to certify equipment and techniques for Federal use to provide authentication/encryption and automated key management for EFTs. Treasury will continue to develop, in conjunction with NBS, automated test beds/bulletin boards so that NBS can validate successful hardware and software implementations of ANSI financial standards.[86]

The Federal Reserve System publicly expressed its commitment to electronic data security in early 1985, when it announced specific plans to enhance its electronic payment services in order to increase their security. The Federal Reserve is a highly-visible participant in the Nation's electronic payments system, both as an operator (performing electronic fund and securities transactions, serving as an automated clearinghouse, etc.) and as a regulator. In its role as an operator, the Federal Reserve must protect its value transactions; as a regulator, the Federal Reserve intends that its security and reliability standards serve as models for depository institutions to emulate in securing their own electronic payments operations.

---

[80] "Information on workshop from David Wilson and Jenny Sobrasky (Ernst& Whinney), private communications with OTA staff May 5-6, 1987, and from an IEEE press release (May 1987).

[81] OTA-CIT-297, op. cit.

[82] Department of the Treasury, Directives Manual, Information Systems Security, Ch. TD 81, Section 40, Apr. 2, 1985.

[83] Department of the Treasury, *Directives Manual*, "Electronic Funds and Transfer Policy—Message Authentication, TD 81, Section 80, Aug. 16, 1984. Superseded by: Department of the Treasury. "Electronic Funds and Securities Transfer Policy–Message Authentication and Endorsed Security, " TD816-02, Oct. 3, 1986, TD/16-02 is authorized by Treasury Order 106-09, Oct. 2, 1986.

[84] Department of the Treasury Order #106-09, "Electronic Funds and Securities Transfer Policy–Message Authentication and Enhanced Security, " Oct. 2, 1986.

[85] J. Martin Ferris, Security Programs, Department of the Treasury, Washington, DC, letter to OTA staff, Dec. 16, 1986.

[86] Ibid.

The Federal Reserve's plans include encryption of depository-institution connections; as of late 1986, over 60 percent of these were encrypted and the Federal Reserve plans to have almost 100 percent of them encrypted by the end of 1987. In addition, the Federal Reserve is currently testing the use of message authentication within the Federal Reserve environment.[87] The National Bureau of Standards is providing technical support to the Federal Reserve.

Technical Standards Development

Technical standards are important for a number of reasons. Among other things, they help to aggregate markets by improving the uniformity, interoperability, and compatibility of vendors' products.

Federal Agency Participation.–NSA and NBS activities in the development of standards have been noted earlier. Other agencies involved in the development and promulgation of regulations and standards include the Office of Management and Budget, the General Services Administration (GSA) and DoD's National Communications System (NCS). GSA promulgates Federal procurement regulations generally, including telecommunications, and has delegated its responsibilities for producing and coordinating communications standards to NCS, which has issued DES-related standards for telecommunications security and interoperability.

NBS has had considerable success during the past decade in developing a variety of standards for information security, as well as by publishing dozens of guidelines. Known as Federal Information Processing Standards (FIPS), NBS standards apply to civilian agencies. Several have also become the basis for standards developed or adopted by NSA and by private standards-setting organizations such as ANSI, the ABA, and the International Organization for Standardization (IS0).

One of the earliest of these national standards, DES, (FIPS 46, released in 1977) is discussed in appendix C. DES, which is now produced in hardware and software both in the United States and overseas,"* has been adopted by ANSI in a number of its technical standards, and was considered for use as an international standard by an IS0 technical committee in 1986, as discussed later.

Private Sector Participation. -Active participation in the development of technical standards for information safeguards is another indication of the current and future needs of business users. ANSI has had active participation from several dozen major corporations, including banks, equipment vendors, and (more recently) other manufacturers. For example, several large U.S. banks and the American Bankers Association (ABA), the Canadian Bankers Association, and about 30 vendors are among the participants in developing standards of interest to the banking community, in addition to NBS, the Treasury Department, and NSA. Suppliers and users of sophisticated safeguards such as biometrics and other technologies not based on cryptography have acted more independently of the Federal Government, sometimes in the absence of technical standards. Defense agencies are major consumers of these products, but the Federal Government does not enjoy the near monopoly in technical expertise that it has in cryptography. In the area of biometrics, the International Biometric Association was formed in 1986 to address industry issues, including establishing a testing and standards program.

Most large corporations have developed or are developing their own information safeguard policies. For example, the Chemical Bank of New York, which has more than 250 branches, has developed its own policies and a security training program for bank employees." The bank's policies, published in 1985,

[87] Jack Dennis, Assistant Director of Federal Reserve Bank Operations, Washington, D.C. Personal communication with OTA staff, Aug. 26, 1986 and letter, Dec. 17, 1987.

[88] Federal Government certification applies only to implementations of DES in electronic devices.

[89] " Corporate Data Security Standards, " Chemical Bank (Chemical New York Corp.), 1985; also Presentation by Joan Reynolds (Chemical Bank), panelist in "Guidelines and Standards Panel, " Ninth National Computer Security Conference, Gaithersburg, MD, Sept. 16, 1986.

define security and custodianship responsibilities in the bank's distributed operating environment and govern the transfer of information in hard copy and electronic forms to protect the bank's information service and data assets. The bank has developed a software package that it uses to train branch officers to perform risk assessments for their local offices and to implement the corporate security standards. By late 1986, the software package had been used in at least 30 Chemical Bank locations.[90]

The Small Business Computer Security and Education Act (Public Law 98-362) provided another mechanism for private sector participation in developing information security standards and guidelines. Passed in July 1984, the act set up a 10-member Small Business Computer Security Advisory Council to advise small businesses on the vulnerabilities to misuse of computer technologies (especially in distributed network environments) and on the effectiveness of technological and management techniques to reduce these vulnerabilities. It also develops guidelines and information to assist small businesses and plans to distribute written materials, including a small business guide to computer security (to be published by NBS) in mid-1987.[91] A report to Congress will be issued by December 1987.

The Applied Information Technologies Research Center (AITRC) represents yet another private sector approach to meeting information safeguard needs. A consortium of scientific, technological, and business organizations based in Columbus, Ohio, AITRC is part of this State-supported program. It was supported by an initial State grant of $1.4 million. Its industrial members include leaders in online information services, and one AITRC project is developing techniques for secure access to private and subscription databases. In the fall of 1986, AITRC was licensing a low-cost, credit card device for remote user identification.[92]

Technical Standards Bodies.—Another indication of the variety of users' needs and demands is provided by the activities of the technical standards-making bodies. Users and vendors in the banking and information processing communities, and in civilian Government agencies, have been working with considerable success for the past decade to develop standards to meet their needs for improved information safeguards. These groups recognize that standards establish common levels of cryptographic-based security and interoperability for communications and data storage systems.[93]

The leading information standards-making organizations in the United States have been the Institute for Computer Sciences and Technology at NBS, the American National Standards Institute (ANSI), and the American Bankers Association (ABA), as noted earlier. The International Organization for Standardization (IS0), develops voluntary standards for international use. Through these bodies, users and vendors are setting the stage for improving the integrity and security of computer and communications systems world-wide.

The American National Standards Institute (ANSI) serves as a national coordinator and clearinghouse for information on U.S. and international standards. It is the central non-government institution in the United States for developing computer, communications, and other technical standards for industry. ANSI

[90] Personal communication between OTA staff and Denise Ulmer, Chemical Bank of New York, Sept. 25, 1986.
The software package, RiskPac™, is also being marketed commercially through Chemical Bank Information Products and Profile Analysis Corporation, Ridgefield, Connecticut. Personal communication between OTA staff and Peter S. Brown, Profile Analysis Corp., Sept. 25, 1986.

[91] Information provided by Peter S. Brown, chairman, Small Business Computer Security Advisory Council, Sept. 25,1986.

[92] Sources: *Information Hotline,* July-August 1986, pp. 6-7; and personal communication between OTA staff and Richard Bowers, AITRC. Sept. 8. 1986.

[93] D Brandstad and M. Smid, "Integrity and Security Standards Based on Cryptography, " North Holland Publishing Co., Computers & Security 1 (1982) CASOO043 [NC]. Also, see Organization for Economic and Co-operative Development, Committee for Information, Computers, and Communications Policy, "Standards and Standard-Setting in Information Technology-Stakes, Strategies, and International Implications, " Sept. 5, 1985.

members represent a broad range of industries and technical disciplines. NBS is a member of many ANSI committees, including those dealing with message authentication and encryption; other Federal agencies including Treasury and NSA also have memberships. ANSI serves as the U.S. representative to the International Organization for Standardization (ISO).

These organizations are structured internally into committees, technical committees, and working groups to accommodate the special interests of their members and to provide a narrow focus, where needed, for developing particular standards and guidelines. Among the structures related to information security are:

- ANSI X3 (Information Processing Systems) Committee, which includes the encryption technical committee; and ANSI X9 (Financial Services) Committee, which includes the financial institution message authentication working group, the financial institution key management committee, and the bank card security working group (focusing on personal identification number, management, and security);
- ABA, which focuses on financial transactions safeguards, including encryption and message authentication; and
- ISO's Technical Committee 97 (TC-97) and its various subcommittees and working groups, which are responsible for developing standards for information processing systems; and Technical Committee 68, which has similar responsibilities for the financial community.

These bodies make extensive use of one another's work, often adopting the other's standard intact or with modifications. Table 10 shows the progress being made in the development of standards and guidelines, as well as many of the contributions of different civilian institutions.

The interests of many developed countries in establishing an international standard for cryptography have recently culminated more than 5 years of deliberation in the IS0. In December 1985, an IS0 technical subcommittee recommended that DES be adopted as an international standard.'}" Any standard adopted by the ISO would likely be used throughout much of the developed world to safeguard communication and computer systems. Disagreements within the U.S. delegation (between NSA and the business community members of ANSI) led the U.S. delegation to abstain during the IS0 vote on DES.[95] ANSI, in mid-1986, recommended to IS0 that cryptographic algorithms not be the subject of international standardization. This change from ANSI's previous position probably came in response to NSA suggestions.[96] Several months later, the IS0 Technical Committee TC97 announced the withdrawal of the proposed DE A-1 standard.[97]

Some of the other nations involved in the IS0 deliberations have proposed their own algorithms as alternatives to DES.[98] This proposal may give credence to what many believe, i.e., that not only can other nations offer encryption algorithms for international use, but that future encryption services will be decided based on international commercial needs. The

[94] Vincent McClellan, "The Pentagon Couldn't Defeat IBM in Battle Over DES Standard, " *Information It 'eek*, Feb. 24, 1986, pp. 24-27.

[95] Ibid., pp. 24-27.

[96] During a meeting with NSA officials in June 1986, OTA staff were advised that since most private sector foreign representatives to the I SO have close ties with their governments, the final ISO decision on whether to adopt the DES could be decided prior to I SO voting through private negotiations among governments. Furthermore, NSA officials have stated that NSA is not in favor of DES (or any one algorithm) being used as an international encryption standard. Harold E. Daniels, Jr., NSA S-0033-87, Feb. 12, 1987, p. 2 of Enclosure 2.

Critics of NSA are sometimes inconsistent. For example, there was speculation that the real reason that NSA opposes DES, or any other algorithm, as an international standard is that it would damage NSA's signals intelligence operations or benefit criminal elements. On the other hand, others speculate that DES is easy for a government intelligence agency to decipher.

However, according to one NSA executive, there is no evidence that anyone has yet found a way to break the DES. But, because DES has come into such widespread use, it may become an attractive target for just such attempts. *OTA* staff meeting with Harold E. Daniels, Jr., NSA, Aug. 13, 1986.

[97] Vincent McClellan, "The Pentagon Couldn't Defeat IBM in Battle Over DES Standard, *information Week*, Feb. 24, 1986, pp. 24-27.

[98] Ibid.

Table 10.—Selected Civilian Technical Standards for Safeguarding Information Systems

Standard/guideline	Developer/year	Principal and other users/uses
Data Encryption Standard (DES) (FIPS PUB 46)	NBS (1977)	U.S. Government (computer and communication security); increasing use in private sector
DES Modes of Operation (FIPS PUB 81)	NBS (1980)	U.S. Government (key management, character transmission, packet transmission, voice)
Key Notarization System (U.S. patent 4,386,233)	NBS (1980)	U.S. Government (notarized identification of originator and receiver of secure message or data file); also used in banks
Guidelines for Implementing the DES (FIPS PUB 74)	NBS (1981)	U.S. Government (general DES user information)
Computer Data Authentication (FIPS PUB 113)	NBS (1985)	U.S. Government (authentication code for data integrity in ADP systems and networks); some use in private sector
Password Usage Standard (FIPS-112)	NBS (1985)	U.S. Government (identifies ten security factors for a password system)
General Security Requirements for Equipment Using DES (FS-1027)	GSA (1982)	U.S. Government (physical and electrical security of DES devices)
Interoperability and Security Requirements of the DES in the Physical Layer of Data Communications (FS-1026)	GSA (1983)	U.S. Government
Data Encryption Algorithm (DEA)	ANSI X3.92 (1981)	U.S. industry (voluntary standard, DEA is ANSI terminology for the DES)
Data Link Encryption Standard	ANSI X3.105 (1983)	U.S. industry
DEA Modes of Operation	ANSI X3.106 (1983)	U.S industry
Financial Institution Message Authentication (wholesale)	ANSI X9.9 (1983)	Wholesale banks (message authentication); industry (electronic procurement message authentication)
Personal Identification Number (PIN) Management and Security	ANSI X9.8 (1982)	Retail banks (DEA encryption of PINs; retailers (computer access control)
Financial Institution Key Management	ANSI X9.17 (1985)	Wholesale banks and industry (cryptographic keys for encryption and message authentication)
Financial Institution Message Authentication (Retail)	ANSI X9.19 (1986)	Retail banks (message authentication using DEA)
Financial Institution Encryption of Wholesale Financial Messages	ANSI X9.23 (draft)	Wholesale banks and industry
Management and Use of PINs	ABA (1979)	Banks (general guidance)
Protection of PINs in Interchange	ABA (1979)	Banks (general guidance)
Key Management Standard Dec. 43	ABA (1980)	Banks (general guidance)
Data Encryption Algorithm (DEA-1)	ISO (1986)	Proposed international version of DES (FIPS-46); withdrawn by ISO Technical Committee TC97.
Modes of Operation of DEA-1	ISO/DIS 8372	Draft international standard has been approved (title may change due to withdrawal of proposed DEA-1 standard)
Data Link Enciphering Standard	ISO/DIS 9160	Draft international standard, version of ANSI X9.105
Message Authentication	ISO/DIS 8730	Draft international standard for message authentication; Part 1 specifies the DEA-1 algorithm, Part 2 specifies the MAA algorithm
Public Key Encryption Algorithm and Systems	ISO/DP 9307	Draft proposal for standards (may be stricken)
Banking: Key Management (wholesale)	ISO/DIS 8732	Draft international standard for wholesale banks

SOURCE Of fice of Technology Assessment, 1987

trend toward the standardization of encryption-based safeguards, principally for improving message integrity (virtually all of which are currently based on DES, often in conjunction with public-key cryptography) suggests that within a few years major segments of the world's businesses will have standardized information safeguards where needed.

Second, these trends indicate that the role of the U.S. Government is shifting from that of the principal developer of safeguard standards in the early 1970s to a more limited role of one participant among many, although with continuing and important responsibilities.

Inherent Diversity of User Needs

Decisions on arcane technical standards, originally based on national security concerns, have already begun to be influenced by various, growing nondefense interests in the United States and worldwide. If safeguard products meeting Federal standards for certification do not fully meet commercial needs, then users are likely to seek greater independence from the Federal Government. Some movement in this direction is already taking place, as evidenced by: unpublicized plans in 1987 of the U.S. banking community to bypass NSA's secret algorithms; growing commercial interest in proprietary public-key algorithms, which have no Federal standard but meet users needs for electronic key distribution and digital signatures; and, the workshop on Integrity Policy for Computer Information Systems, planned for late 1987, which will focus on military v. commercial security models.

The foregoing description of various users' needs, and actions that Government and private sector groups have undertaken to meet them, serves to point out the inherent diversity and heterogeneity of users' needs for information safeguards. Within the Federal Government itself, for example, different requirements exist among defense and civilian agencies, and even between classified and unclassified applications (such as food service or routine procurement) within DoD. The private sector is no more uniform in its needs, attitudes, and perceptions. In order to understand the differences in each user's requirements, priorities, and perceived risks and threats, information such as the following must be evaluated by each user:

- What are the user's major concerns? For example, what is the relative priority for various types of information for integrity versus confidentiality, versus reliability and continuity of service?
- What sensitive information may warrant better safeguards than are now provided?
- Who are the adversaries that need to be protected against (employees, competitors, foreign governments) and the resources they are likely to use?
- What are the likely consequences (financial, embarrassment, privacy) of different types of losses? What has been the loss experience to date?
- What are the decision criteria (costs and benefits for bolstering safeguards, required by law, risk aversion)?

Responses to these and other questions help to define the user's needs for safeguards and are likely to be different from one user to another, even when they are in the same general business. A defense contractor bound by DoD policies and regulations for safeguarding classified information from foreign adversaries, for example, can recover the costs of safeguards from the Government. This is a very different situation than that of a large retailer who needs to authenticate thousands of transactions per day, with emphasis on service delivery, costs, data integrity, and protection against dishonest employees and customers. And, the retailer's needs bear little resemblance to the bank manager's requirement to show that he has exercised due care in safeguarding the bank's assets.

Chapter 6 focuses on some of the major laws and policy directives concerning information security. In tracing the development of public policy, it seeks to provide insights into the question: "How did we get where we are today?"