Chapter 6

Major Trends in Policy Development

CONTENTS

Tables

Chapter 6

Major Trends in Policy Development

FINDINGS

- Federal policy limiting the disclosure of information has expanded over the last decade to include growing concern for protecting unclassified, but sensitive information, such as that in commercial and Government databases. As part of this process, the role of the defense and intelligence communities has also expanded and "national security," as a criteria for non-disclosure, is being interpreted more broadly.
- Federal policies on information security are creating tensions with broad national interests and, in contrast with earlier times, can no longer be isolated from them.
- Most recent Federal policies on information security are based principally on national security concerns. Now that information security is becoming important to commerce, more broadly based policies will be more appropriate.
- The National Security Agency (NSA), in carrying out its role under National Security Decision Directive (NSDD-145) to develop computer and communications security standards for use by Government and industry, is involved in two policy conflicts. One conflict involves responsibilities for developing security standards, with the National Bureau of Standards (NBS) charged by the Brooks Act of 1965, as amended, and NSA having overlapping responsibilities under NSDD-145. The second is a continuing, inherent conflict between NSA's mission to perform signals intelligence and its efforts to develop computer and communications safeguards for widespread nondefense use.

INTRODUCTION

Policy for the security of electronic information has developed in recent years in a setting of diverse interests. These interests have included national security and the separation of powers for governmental policymaking, as well as civil liberties, including personal privacy, and commercial needs for improved information safeguards. The current tensions in information security policy reflect all of these influences. To a large extent, these tensions have their basis in different views within Government of overall national interests and the central historical role of the Government, particularly the Department of Defense (DoD), in developing technology and setting policies for safeguarding electronic information.

This chapter provides a brief review of two of these influences:

- the context of Government controls on unclassified information that has evolved during the past few decades, and;
- the progression of prior policies concerning the privacy and security of electronic information that have led to today's policies.

Policies designed to keep electronic information secure developed historically largely in the context of protecting national security. One of the important ways that has been used to limit potential damage to the nation's security is through controls on the dissemination

of information. Federal limitations, dating to before the turn of the century, sought to prevent the disclosure and distribution of militarily sensitive, Government-owned or -controlled information. [1]

Traditionally, information protected for national security reasons has been limited to military and diplomatic categories. Since the 1940s, a number of laws have been passed and presidential directives issued that have gradually expanded the range of information deemed vital to U.S. national security. Controls have been placed on data relating to, for example, atomic energy, space programs, and a variety of other technologies. (See table 11.) Similarly, efforts have been made to keep intelligence sources and methods secret and there have been discussions on whether controls might be warranted for satellite imagery gathered for the news media.[2]

At the same time, the medium of information that is to be controlled—i.e., oral, print, photographic, or electronic—has also expanded. The setting for the transfer of controlled information has become irrelevant, whether through the export of products or services, sales presentations, university laboratories and classrooms, or scientific or trade conferences.

Against this backdrop, computer and communications systems are among the media for controlling the transfer of such sensitive information. Concern for their vulnerability to penetration, particularly by foreign intelligence entities, has resulted in pressure to increase the security of these systems.

A second context that affects Government controls on information concerns the respective roles of and occasional conflicts between the executive and legislative branches in setting policy when national security is at stake.[3] The history of this controversy has its origins in the drafting of the Constitution and it continues to raise complex issues for both branches. Since the beginning of the Cold War in the mid-

Table 11.—Selected Government Policies Related to Controls on Information Flows: A Context for Electronic Information Security

1940s:
- Atomic Energy Act[a]
- Export Control Act[b]
- National Security Act[c]
  —establishes the Central Intelligence Agency

1950s:
- Invention Secrecy Act[d]

1960s:
- Export Administration Act of 1969e

1970s:
- Arms Export Control Act of 1976f
- PD/NSC-24[g]
  —safeguard sensitive Government information in communications systems

1980s:
- Defense Authorization Act, 1984h
  —controls, on military and space technical data
- NSDD 189[i]
  —clarify controls on basic research data
- NSDD 145[j]
  —safeguard sensitive information in computer and communications systems

Recent reports:
- Air Force study of foreign access to commercial databases
- Soviet acquisition of Western technology[k]
- Senate report on counterintelligence[m]

[a] Atomic Energy Act of 1946 (60 Stat 755).
[b] Export Control Act of 1949 (63 Stat. 7)
[c] National Security Act of 1947 (50 U S C. 403, Sec. 403). This Act also provides standards for classifying and safeguarding Information for the protection of national security, notably Intelligence sources and methods
[d] Invention Secrecy Act of 1951 (U S.C. 181-188).
[e] Export Administration Act of 1979 (50 App USC 2401.2413). as amended 1979 1981, 1985.
[f] Arms Export Control Act of 1976 (22 USC 2571 et seq.)
[g] Presidential Directive/National Security Council-24, (PD/NSC 24), Telecommunications Protect Ion Policy (unclassified excerpts, dated Feb 9. 1979), Nov 16 1977 (classified)
[h] Department of Defense Authorization Act, 1984, P L 98-94, SePt 241983 Section 1217, Authority to Withhold from Disclosure Certain Technical Data (10 U.S C 140c)
[i] NSDD 189, National Policy on the Transfer of Scientific, Technical, and Engineering Information, Sept 21, 1985
[j] National Security Decision Directive 145 (NSDD 145), Policy on Telecommunications and Automated Information Systems Security, Sept 17, 1984
[k] "The Exploitation of Western Data Bases," Report of the Air Force Management Analysis Group, (Secret), June 30, 1986
[l] Soviet Acquisition of Militarily Significant Western Technology An Update, " Department of Defense, September 1985
[m] Meeting the Espionage Challenge," Senate Select Committee on Intelligence, Report No 99-522, Oct 3, 1966

[1] "The Evolution and Organization of the Federal Intelligence Function: A Brief Overview (1776-1975)," Supplementary Reports on Intelligence Activities, Book 6, Senate Select Committee to Study Government Operations, Report 94-755, Apr. 23, 1976.

[2] U.S. Congress, Office of Technology Assessment, *Commercial Newsgathering From Space—Technical Memorandum, OTA-TM-I SC-40* (Washington, DC: U.S. Government Printing Office, May 1987).

[3] Harold C. Relyea, "National Security and Information, " *Government Information Quarterly,* vol. 4, No. 1, 1987, pp. 11-28.

1940s, the debate over the roles of the two branches has included such topics as atomic energy, satellite communications, and the funding of research in fields such as electronics and supercomputers and of the roles of the military v. civilian agencies.

The controversy over policymaking responsibilities within the Federal Government has a direct bearing on Federal policy in information security primarily because it influences the scope of national interests to be embraced in such policies and, in that process, the priorities emphasized. For example, one view of national interests places priority on military advantage and defense capability, with national security often being promoted through reliance on secrecy and Government controls. Advocates of this view accept the idea of Government control of access to information in the greater interest of national security. The other viewpoint focuses on the United States as a free and open society in which access to information, for realizing scientific, economic, and intellectual achievement, should be subject to only minimal Government control when there is clear justification.

In addition, the process by which policy is developed is becoming increasingly important as the range of national interests affected expands beyond national security concerns and, consequently, as tensions among competing objectives are created. Policymaking in Congress tends to be an open process, in contrast with the often closed process underlying past executive branch policies concerning communications and computer security.

Federal policy on electronic information security has also been shaped by concerns for privacy and civil liberties. Laws have been passed limiting warrantless Government wiretaps and prohibiting eavesdropping on others' private communications or gaining unauthorized access to computer systems. This path of Federal policymaking, which has its origins with the Communications Act of 1934, has gained momentum during the past two decades independent of concerns for foreign intelligence gathering.

As a consequence of these various influences, most of which have ramifications that extend well beyond information security, policy formulation has followed at least two interdependent paths, at times initiated by Congress and at other times by the executive branch. The resulting policies, are highlighted in table 12. In this process, however, there has been a growing influence of defense and intelligence interests in shaping policy for the security of unclassified electronic information.

Until recently, Federal policies on electronic information security, whatever their objectives, have not raised tensions. What is different about the policies of the 1980s, however, is that some of these have begun to affect segments of the private sector more significantly. In contrast with earlier policies, which had negligible influence on nondefense businesses or private citizens, recent policies have tended to impose added burdens on some businesses, to raise concerns for new restrictions on private sector access to unclassified, but sensitive information, and to interject an intelligence agency in normal business operations. (See ch. 5.)

Some of the key questions that arise are: where is policy for the security of electronic information leading? can the current issues be resolved? what new issues might arise? The review of the evolution of policy in the remainder of this chapter provides limited insights into the answers to these questions. For example, there is little indication that any permanent change is about to occur to reconcile the different views of the national interest and how these should be addressed in policy on the security of electronic information. It is more likely, given the complexity of the issues, that the narrower ones will be addressed, such as the extent of controls on information flows v. the ease of public access to Federal information intended by the Freedom of Information

Table 12.—Government Actions Affecting the Security of Information in Computer and Communications Systems

	Executive Branch	Legislative Branch	Key Reports
World War I	War Department[a]		
Post World War I	American Black Chamber[b]		
1934		Communications Act[c]	
1952	NSA created[d]		
1965 ., ...		Brooks Act[e]	
1968		Omnibus Crime Control and Safe Streets Act[f]	
1976			Senate report on Federal intelligence functions
1977	NBS establishes DES as U.S. standard		MITRE reports on communications security[h]
1978		Foreign Intelligence Surveillance Act[i]	
1979	Policy on protection of government communications, PD/NSC-24[j]		RAND report on computer security[k]
1980			NTIA White Paper[l]
1981	Executive Order 12333[m]		
1984	Policy on protection of government computer and communications systems, NSDD 145. [n]		
$985		House hearings on computer security policy[o]	
1986	Policy on protection of sensitive information	HR 145, Computer Security Act[p]	
	NSA decision to replace DES	Computer Fraud and Abuse act[r]	
		Electronic Communications Privacy Act[s]	
1987	Planned review of NSDD[q]	House hearings on HR 145[t]	House report on computer security[u]

[a] Responsibilities of the War Department included safeguarding classified and diplomatic messages and signals intelligence operations
[b] H. O. Yardley, *The American Black Chamber*, Bobbs-Merrill Co., Indianapolis, 1931. As reported in David Kahn, *The Codebreakers*, pp. 360-361
[c] The Communications Act of 1934, Section 605 (now section 705), as amended
[d] The National Security Agency was created by a still-classified presidential memorandum in 1952. NSA's responsibilities include safeguarding Government classified and diplomatic communications and foreign signals intelligence operations
[e] Public Law 89-306
[f] Title 3 of the Omnibus Crime Control and Safe Streets Act of 1968 protects the privacy of wire and oral communications and delineates conditions under which interception of wire and oral communications may be authorized
[g] "The Evolution and Organization of the Federal Intelligency Function: A Brief Overview (1776-1975)," Supplementary Reports on Intelligence Activities, Book VI. Senate Select Committee to Study Government Operations, Report 94-755, Apr. 23, 1976
[h] "Study of the Vulnerability of Electronic Communications Systems to Electronic Interception," Volumns 1 & 2, the MITRE Corp., January 1977; "Selected Examples of Possible Approaches to Electronic Communications Intercept Operations," the MITRE Corp., January 1977. These reports were prepared under contract to the Office of Telecommunications Policy, Executive Office of the President
[i] Public Law 95.511 establishes standards and procedures for the use of electronic surveillance for Government intelligence collection within the United States, including wiretaps and radio interception
[j] Presidential Directive/National Security Council-24 (PD/NSC-24) Telecommunications Protection Policy (unclassified excerpts, dated Feb. 9, 1979), Nov. 16, 1977 (classified)
[k] "Security Controls for Computer Systems," Report of the Defense Science Board, Task Force on Computer Security. Originally published as a classified document (R-609), February 1970. Republished as R-609-1 by the RAND Corp., October 1979 (unclassified)
[l] "Analysis of National Policy Options for Cryptography," National Telecommunications and Information Administration, Department of Commerce, Oct. 29, 1980
[m] Executive Order 12333, United States Intelligence Activities, Dec. 4, 1981. The order includes a description of certain authorities of NSA for communications security safeguards.
[n] NSDD 145, Policy on Telecommunications and Automated Information System Security, Sept. 17, 1984, assigns responsibility for computer and communications security to a single executive agent, the Secretary of Defense, and a single national manager, the Director of NSA
[o] Hearings on computer security policies, House Subcommittee on Transportation, Aviation, and Materials, Committee on Science and Technology, June 27, 1985
[p] The Computer Security Act of 1986 (now 1987), HR 145.
[q] Policy on protection of Sensitive, but Unclassified Information in Federal Government Telecommunication and Automated Systems, NTISSP No. 2, Oct. 29, 1986. This policy provides a definition of such sensitive Information and notes the responsibilities of department heads for deciding when safeguards are warranted. This policy was rescinded in March 1987 by Frank Carlucci, Chairman, National Security Council, and at the same time, a review of NSDD 145 was ordered
[r] Public Law 99-474 provides penalties for unauthorized access to certain financial records in computer systems and for trespassing on Federal computers
[s] Public Law 99-508 amends Title 3 of the Omnibus Crime Control and Safe Streets Act of 1968 it protects against the unauthorized interception of electronic communications
[t] Hearings on HR 145 of the House Subcommittee on Legislation and National Security, Feb. 25-26, and Mar. 17, 1987, and joint hearings of the House Subcommittee on Transportation, Aviation and Materials, Feb. 26, 1987
[u] House report 100-153, Parts 1 and 2, June 11, 1987, 100th Cong., 1st Sess.

Act, and the appropriate roles of NSA v. NBS in providing safeguard standards for non-defense use.

Finding an appropriate balance between these different views is not easy. Both are embodied in laws and policies, and both have strong advocates within and outside Government. Moreover, they have an existence that transcends the current debate over information security. Still, the issues raised by the debate demand attention now because of the implications of information security for the conduct of government, business, science, and our personal lives.

Two important shifts appear to be occurring, however. The first is a wider recognition of the impacts of policies on users of information security products and on providers of information services, particularly where the public does not understand or agree with the need for controls, or where impacts fall unevenly. The second major shift, one that is still being deliberated, is a reluctance by Congress to accept executive branch policies on information security when they require subordinating other important national interests. These two trends suggest that future policies for national security will have to be integrated with other interests, or alternative means found for satisfying them, such as through the technological and administrative safeguard measures noted in chapters 4 and 5.

THE EVOLUTION OF FEDERAL POLICY FOR SAFEGUARDING UNCLASSIFIED INFORMATION IN COMMUNICATIONS AND COMPUTER SYSTEMS

Executive Branch Activities in Information Security

Government policies have focused on the confidentiality of electronic communications since before World War I.[4] These policies provided the means for protecting classified defense and diplomatic messages transmitted over Government and commercial communications systems. For most of this century, U.S. policies included both communications security and signals intelligence operations against foreign governments.[5] These functions became dispersed within each of the military departments, but were consolidated with the creation of the National Security Agency (NSA) within DoD in 1952.[6]

While U.S. defense agencies have long had an interest in preventing Soviet acquisition of various militarily useful equipment produced in this country or by our allies, they have also begun of late to urge export protection of technical information that could be used for military or commercial purposes. Consequently, in some policy circles, the concept of national security, which in times past was very familiar to our understanding of "national defense and foreign policy," has taken on a broader meaning, one encompassing a wide range of economic, technical, scientific, and business information.

At the same time, two other concerns have arisen. One is over Soviet and other countries' electronic intelligence gathering in the United States. A second involves an increase in the range of potential international adversaries. No longer are they perceived as limited to military and diplomatic opponents, but include economic rivals as well as terrorists, drug traffickers, and organized crime.

From such considerations have come an increasing interest in protecting information

[4] For an account of early Government intelligence operations, including wiretapping, codemaking, and codebreaking, see: Supplementary Reports on Intelligence Activities, Book 6, Final Report of the Select Committee to Study Government Operations with respect to Intelligence Activities, U.S. Senate, Report No. 94-'755, Apr. 23, 1976.

[5] James Bamford, *The Puzzle Palace (New* York, NY: Penguin Books, 1983), p. 206. The Army's cryptologic capability dates at least to World War 1.

[6] Ibid., p. 81. NSA was created by a top secret presidential order signed by President Harry S Truman on Oct. 24, 1952.

that, although not classified, is nevertheless important or sensitive enough alone or in combination with other unclassified information to warrant special precautions. As a consequence, anew category of unclassified, but sensitive information has developed.

Computer Security

Executive branch interest in computer security began with the establishment of a task force in 1967 to recommend safeguards to protect classified information in multi-access, resource-sharing computer systems. The work of the task force, which was sponsored by DoD's Defense Advanced Research Projects Agency, resulted in a classified report issued by the Defense Science Board in 1970, a declassified version of which was published in 1979.[7]

At the same time, NSA, which **was concerned** about the vulnerability of the U.S. banking system, began encouraging NBS to become involved in computer security. Based on the authority of the Automatic Data Processing Equipment Act (widely known as the Brooks Act) of 1965,[8] NBS was already developing performance standards for computers used by the Federal Government. As a result, NBS and the Association of Computing Machinery cosponsored a conference in 1972 on computer security. Following the conference, NBS initiated a program in computer and communications security in 1973 based on the Brooks Act. This program led to the adoption in 1977 of the Data Encryption Standard (DES), as a national standard for cryptography. (See ch. 4.)

Since then, NBS has published dozens of Federal Information Processing Standards and guidelines, validated commercial encryption devices, participated in voluntary standards groups, assisted other civilian agencies, and, with NSA, cosponsored annual conferences on computer security. NBS also works with users and vendors in developing many of their products. Recently, the agency has contributed to the development of standards for network security as part of the 'open system interconnection network. "

The 1970 task force report also prompted DoD to improve the security of classified information in computer systems. Research and development undertaken by the Air Force, Defense Advanced Research Projects Agency, and other defense agencies in the early- and mid- 1970s demonstrated approaches to technical problems associated with controlling shared-use computer systems.[9]

As a result of these activities, DoD launched the Computer Security Initiative in 1978, a program largely transferred to NSA in 1981, to address the department's computer security needs. The program became the National Computer Security Center (NCSC) in 1984 with the issuance of NSDD-145. NCSC develops standards and guidelines, evaluates computer hardware and software security properties, undertakes research and development, and trains users. According to NCSC literature, the center addresses the Nation's computer security problems rather than just those associated with classified information or defense agency requirements.

Many of NCSC's activities affect civilian agencies and the private sector. Among these are the development of criteria for evaluating the security of trusted computers, known as the "Orange Book. "]" NCSC, or other parts of NSA, rate commercial products based on the orange book criteria and train people in computer security, evaluate commercial DES products and other cryptographic devices,[11] de-

[7]Security Controls for Computer Systems, Report of Defense Science Board Task Force on Computer Security, Office of the Secretary of Defense. Originally published as a classified document (R-609), February 1970; republished as an unclassified document {R-609-1), October 1979, by the RAND Corp., Willis Ware, editor.

[8]Public Law 89-306, Automatic Data Processing Equipment Act of 1965.

[9]J. P. Anderson, "Computer Security Technology Planning Study, " ESD-TR-73-51, vol. I, AD-758 206, ESD/AFSC, October 1972.

[10]Department of Defense Trusted Computer System Evaluation Criteria, DoD 5200.28 -STD, December 1985. See also CSC-STD-001-83, Aug. 15, 1983.

[11]Under the Commercial Communications Security Endorsement Program.

sign cryptographic modules for vendor manufacture, and develop secure telephone equipment. NCSC also publishes standards and guidelines for computer security and participates in voluntary standards activities with industry. (See ch. 5.)

Communications Security

PD/NSC-24

Increasing concern during the mid-1970s about Soviet interception of unclassified U.S. domestic communications led to a change in executive branch policy. Presidential Directive/National Security Council-24 (PD/NSC-24) was signed by President Jimmy Carter in 1977. It expanded the authority of DoD and, in a more limited way, the Department of Commerce, for safeguarding unclassified, but sensitive communications that "would be useful to an adversary.[12]" PD/NSC-24 directed Federal department heads to protect unclassified, but sensitive communications. It assigned responsibility to DoD for the security of classified communications and for unclassified, but sensitive communications related to national security. It also assigned responsibility to the Department of Commerce for raising users' awareness of the vulnerability to interception of communications systems. In addition, PD/NSC-24 charged the Defense and Commerce Departments with developing a joint proposal for a national policy on cryptography. DoD's responsibilities were carried out by NSA and Commerce's National Telecommunications and Information Administration (NTIA).

Several DoD directives were issued to implement PD/NSC-24. The first, National Communications Security Council Policy-10 (NCSC-10),[13] called for the protection of sensitive information transmitted by the Government or DoD contractors over satellite links. It was followed by NCSC-ll,[14] which broadened NCSC-10 to protect all transmission systems carrying sensitive information from Government and DoD contractors. Neither NCSC-10 nor NCSC-11 included a funding mechanism, but NSA issued National Communication Security Instruction 6002 in 1984.[15] It authorized Federal agencies and Government contractors to purchase approved equipment and services to protect unclassified, but sensitive information. (See ch. 5.) For its part, NTIA conducted seminars on communications vulnerabilities for more than 1,500 Federal employees.

DoD and Commerce were not able to develop a joint proposal for a national policy on cryptography, however, because of disagreements over compromises concerning national security, trade, innovation, and First Amendment rights. Instead DoD and Commerce submitted separate proposals. Essentially, the DoD proposal called for a continuation of various Government controls on cryptography, such as on patents and the export of equipment and technical data, while Commerce proposed minimizing these controls and argued for greater sensitivity to the negative effects they have on broader national interests.[16]

The NTIA effort under PD/NSC-24 was hindered significantly by the absence of definitions of the terms "sensitive information and "useful to a foreign adversary" that could serve as practical guides to department heads. This shortcoming is significant because the broad definition provided in NSDD-145 later had to be withdrawn due to public apprehension about its potentially wide applicability.

[12]Presidential Directive/National Security Council-24 (PD/NSC-24), Telecommunications Protection Policy (unclassified excerpts, dated Feb. 9, 1979), Nov. 16, 1977 (classified).

[13]National Policy for the Protection of U.S. National Security Related Information Transmitted over Satellite Systems, NCSC-10, Apr. 26, 1982. The National Communications Security Council was a predecessor organization to that established under NSDD-145.

[14]National Policy for Protection of Telecommunication Systems Handling Unclassified National Security Related Information (NCSC-1 1), May 3, 1982.

[15]Protection of Government Contractor Telecommunications, National Communication Security Instruction 6002 (NACSI-6002), June 1984.

[16]This assessment stems from OTA staff interviews in April 1987, with former NTIA officials involved in developing the Department of Commerce proposal for a national policy on cryptography. Also, see "White Paper: Analysis of National Policy Options for Cryptography, " National Telecommunications and Information Administration, U.S. Department of Commerce, Oct. 29, 1980.

PD/NSC-24 had at least two notable effects: it pioneered an experiment by assigning some limited responsibility for safeguarding Government communications to a civilian agency —the Commerce Department-and it provided authority for NSA to protect unclassified communications. The assignment to NSA was the beginning of a trend toward consolidating and broadening responsibilities for the security of unclassified electronic information within DoD.

The joint Defense and Commerce programs, begun in 1978 under PD/NSC-24, were short-lived. They ended when NTIA's involvement was discontinued in 1982 due to reasons of general agency budget reductions. Further, PD/NSC-24 itself was superseded by NSDD-145 in 1984. Many of the activities initiated under PD/NSC-24 now come under the authority of NSDD-145.

NSDD-145

The current national charter for information security is provided by Executive Order 12333[17] and National Security Decision Directive 145 (NSDD-145). Executive Order 12333 assigns to the Secretary of Defense responsibility for making Government communications secure.

NSDD-145 is the current fundamental policy for communications and computer security. It:

- recognizes the merging of communications and computer technology and is intended to direct a coordinated approach to securing both types of systems;
- continues the emphasis on protecting unclassified, but sensitive information begun under PD/NSC-24;
- assigns responsibility for computer and communications security solely to a single executive agent, the Secretary of Defense, and a single national manager, the Director of the National Security Agency; and
- establishes a specific responsibility for major Government resources to be used to "encourage, advise, and if appropriate assist the private sector to protect against exploitation of communications and automated information systems.

NSDD-145 states that telecommunications and automated information systems "are highly susceptible to interception, unauthorized electronic access, and related forms of technical exploitation, as well as other forms of hostile intelligence threat. " It recognizes that exploitation can occur from terrorist groups and criminal elements, and that private or proprietary information can become targets for foreign exploitation. NSDD-145 focuses on unclassified, but sensitive electronic "Government and Government-derived information, the loss of which could adversely affect the national security interest. "

The directive establishes an interagency organization that includes virtually all Federal defense, intelligence, and law enforcement, as well as some civilian agencies. The leadership of the interagency group is also responsible for the security of classified information.

The organizational structure is shown in table 13. The key points to note are:

- The Systems Security Steering Group *oversees* the implementation of NSDD-145. It is composed of the secretaries of State, Treasury, and Defense, the Attorney General, the director of the Office of Management and Budget, and the director of the Central Intelligence Agency, and was chaired by the President advisor for National Security Affairs as recently as 1987.
- Working under the steering group's guidance is the National Telecommunications and Information Systems Security Committee (NTISSC), which develops operating policies and provides security guidance to Government agencies. NTISSC is composed of representatives of Government agencies and departments having principle or major missions in military, intelligence, and law enforcement, among others. It is chaired by the assistant sec-

[17] Executive Order 12333, United States Intelligence Activities, Dec. 4, 1981.

Table 13.—Committees Guiding the Implementation of NSDD 145

Systems Security *Steering Group:*
1. Secretary of State
2. Secretary of the Treasury
3. Secretary of Defense[a]
4. Attorney General
5. Director of OMB
6. Director of Central Intelligence[a]
7. Assistant to the President for National Security Affairs, chair[a]

National Telecommunications and Information Systems Security ***Committee:***

Consists of a voting representative of each of the above, plus a representative designated by each of the following:

8. Secretary of Commerce
9. Secretary of Transportation
10. Secretary of Energy
11. Chairman, Joint Chiefs of Staff[a]
12. Administrator. GSA
13. Director, FBI
14. Director, Federal Emergency Management Agency
15. Chief of Staff, Army[a]
16. Chief of Naval Operatlons[a]
17. Chief of Staff, Air Force[a]
18. Commandant, Marine Corps[a]
19. Director, Defense Intelligence Agency[a]
20. Director, National Security Agency[a]
21. Manager, National Communications System[a]
22. Assistant Secretary of Defense for Command, Control, Communications, and Intelligence, chair'

[a]Denotes a representative closely associated with the de fense/nati on al secu nty community

SOURCE Donald C Latham Assistant Secretary of Defense Command. Con trolCommunications and Intelligence, testimony before the House Subcommittee on Transportation Aviation, and Materials and Subcom- m I ttee on Sc I ence Research, and Technology Feb 26 1987 See also NSDD 145 Sept 17 1984

retary of defense (for command, control, communications, and intelligence).

- The interagency group's executive agent for telecommunications and information systems security is the Secretary of Defense, who approves standards and doctrine, and reviews the security budgets of other departments and agencies.
- The national manager for telecommunications and automate-d information systems security is the director of NSA, who serves as the Government focal point for cryptography, telecommunications, and automated information systems security, conducts R&D for security, and approves all standards, techniques, systems, and equipments for the security of these systems.

Critics of NSDD-145 have charged that the organization is dominated by defense and intelligence interests and that the National Security Council, as chair of the steering group, acts in a decisionmaking capacity rather than as an advisor to the President. They also charge that NSDD-145 raises a conflict by giving authority to NSA to develop standards for computer security, authority that was previously given to NBS under the Brooks Act. The conflict has caused manufacturers and business users of information security products to question which Government agency has leadership for standards development, equipment endorsement, and related functions, and raised the issues of the appropriate division of responsibility between civilian and military agencies, as well as the secrecy and absence of open accountability of NSA.

Definition of Sensitive Information

Finally, there has been considerable concern over public access to unclassified, but sensitive information (see below). One main reason was the definition of the term as information whose loss, misuse, alteration, or destruction "could adversely affect national security or other Federal interests. These national security interests were defined as:

> ,.. matters that relate to the national defense or the foreign relations of the U.S. Government. Other Government interests are those related, but not limited to the wide range of Government or Government-derived economic, human, financial, industrial, agricultural, technological, and law enforcement information, as well as the privacy or confidentiality of personal or commercial proprietary information provided to the U.S. Government by its citizens. [18]

Shortly after this definition was issued, Diane Fountaine, director of information systems for the Office of the Assistant Secretary of Defense, Command, Control, Communications and Intelligence, spoke before the Information Industry Association in New York City on November 11, 1986. This official was widely quoted as saying:

"National Policy on Protection of Sensitive, but Unclassified Information in Federal Government Telecommunications and Automated Systems, NTISSP No. 2, Oct. 29, 1986.

> I don't believe that the issue is whether or not we [DoD] are going to protect information. I really believe that the issue is what information we are going to protect, both from the Federal Government, both within DoD and also within industry. [19]

The overall statement was apparently intended to assure listeners that the restrictions would apply to Soviet access to U.S. databases and not to the U.S. scientific and technical community. Nevertheless, it was generally seen as foreboding by those who fear further Federal restrictions on unclassified information.

At about the same time, two other related events were publicized that reinforced concerns for Government restrictions on unclassified information. One involved reports of a classified Air Force study on foreign access to databases in the United States and other Western countries, and what can be done to limit such access. [20] The other involved well-publicized visits to commercial database firms by representatives from the Federal Bureau of Investigation, Central Intelligence Agency, and NSA asking how controls might be placed on subscribers to their systems. These visits received considerable publicity by the news media.

Policy Development in Congress

While passing legislation that provided the legal basis for some Government controls on information, Congress has also sought to protect the confidentiality of electronic communications and computer information as well as individuals' rights and privacy. The laws identified below illustrate this trend, which has been occurring simultaneously and parallel to executive branch directives aimed at national security concerns. Still other laws, not shown, protect the privacy of individuals, such as the Privacy Act and the Fair Credit Reporting Act.

The Communications Act of 1934, Section 605 (now Section 705), as amended, provides that "No person not authorized by the sender shall intercept any communications and divulge. . . the content. " Notwithstanding this legislation and the 1938 Supreme Court interpretation (Nardone v. United States, 302 U.S. 379) that Section 605 prohibited all telephone wiretapping even when done by Federal Government officers, Government wiretapping continued. [22]

Title III of The Omnibus Crime Control and Safe Streets Act of 1968 includes sections that protect the privacy of wire and oral communications, and delineate on a uniform basis the circumstances and conditions under which the interception of wire and oral communications may be authorized.[23]

The Foreign Intelligence Surveillance Act of 1978 (Public Law 95-511) establishes legal standards and procedures for the use of electronic surveillance in collecting foreign intelligence and counterintelligence within the United States. Electronic surveillance is defined to include wiretaps, radio intercepts, and other forms of surveillance.[24]

The Electronic Communications Privacy Act of 1986 (Public Law 99-508) protects against the unauthorized interception of electronic communications. It amends Title III of the Omnibus Crime Control and Safe Streets Act of 1968. The Electronic Communications Privacy Act addresses three limitations in Title III protection that had developed as a result of technological changes.[25] The limitations concern the "aural acquisition" of oral Communications (in contrast with the acquisition

[19] Draft transcript of speech by Diane Fountaine's presentation at the Information Industry Association Annual Convention, Nov. 11, 1986. Transcript provided by the Information Industry Association. See also "Pentagon Weighs Data Bank Curbs, " *New York Times*, Nov. 11, 1986.

[20] Op. cit., Fountaine statement.

[21] " Pentagon Weighs Data Bank Curbs, " New York Times, Nov. 12, 1986; "Are Data Bases A Threat to National Security?" *Business Week,* Dec. 1, 1986.

[22] U. S. Congress, Office of Technology Assessment, *Federal Government Information Technology: Electronic Surveillance and Civil Liberties, OTA-C IT-293* (Washington, DC: U.S Government Printing Office, October 1985), p. 18.

[23] 1 bid., pp. 18-21.

"Ibid., pp. 20-21.

[25] For a more thorough discussion of technological changes and the legal protections for the privacy of communications see: *Federal Government Information Technology: Electronic Surveillance and Civil Liberties, OTA-C IT-293,* op. cit., October 1985.

of digital communications), Communications over nonwire facilities, and communications over systems other than public telephone systems.

The Electronic Communications Privacy Act of 1986 extends legal protection in each of these areas. It prohibits unauthorized interception of video and data communications. It defines "electronic communication" to include "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature. Exceptions to this include the radio portion of a cordless telephone communication, any communication made through a tone-only paging device, and any communication made through a tracking device, such as is used for electronic surveillance. The 1986 act also extends protection to communications transmitted "in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system. "

Communications also are protected against intentional interception regardless of the means by which they are transmitted. But the inadvertent reception of satellite transmissions or radio communications is not penalized. The Electronic Communications Privacy Act also protects against the disclosure of stored wire and electronic communications (e.g., electronic mail records) and provides legal standards for access to the transactional records of communications providers. These extended protections address some of the vulnerabilities of communication systems identified in chapters 3.

The Computer Fraud and Abuse Act of 1986 (Public Law 99-474) provides penalties for unauthorized access to certain financial records in computer systems, including a 5-year felony provision for unauthorized access to a "Federal interest computer" with an intent to defraud. It also provides for a penalty for intentional trespassing on Federal computers. The act establishes a felony provision for malicious damage to a Federal interest computer and a misdemeanor provision for posting passwords on "pirate bulletin boards. [26]

[26] "Public Law 99-474, The Computer Fraud and Abuse Act of 1986, signed into law Oct. 16, 1986. Computer Crime and Security, Issue Brief, Congressional Research Service, 11385155, Mar. 10, 1987.

GOVERNMENT CONTROLS ON UNCLASSIFIED INFORMATION

Controls Through Legislation

At the same time that it sought to protect individual rights and privacy from Government and other intrusions, Congress also gave the executive branch authority to limit public access to certain kinds of information, both classified and unclassified. A series of laws were enacted that gave the President and certain department and agency heads power to withhold information to protect its secrecy and to restrict access to it.

The Atomic Energy Act of 1946 (60 Stat. 755). One of the Federal Government's oldest mechanisms for controlling scientific communications, the Atomic Energy Act of 1946, had its origins in the rigid secrecy surrounding the World War II Manhattan Project and the Government monopoly on atomic energy research and development. [27] The Atomic Energy Act created the category of Restricted Data, which it defined as "all data concerning (1) design, manufacture or utilization of atomic weapons; (2) the production of special nuclear material; or (3) the use of special nuclear material in the production of energy. " A revised version, enacted as the Atomic Energy Act of 1954 (68 Stat. 919; 42 U.S.C. 201 1-2296), permitted access and retention to some Restricted Data by private firms engaged under license in industrial applications of nuclear power, provided that they obtained the necessary security clearances and abided by the required information controls.

[27] U. S. Congress, House Committee on Government Operations, "The Government's Classification of Private Ideas, " House Report *96-1540.* 96th Cong., 2d sess., Dec. *22,* 1980.

Without explicitly using the phrase "born classified," the Atomic Energy Act provides that Restricted Data is subject to secrecy from the moment of its creation, even though the creator may be a private individual. The Government has taken legal action against private parties, most notably The *Progressive* magazine, which was planning to publish an article (based on declassified, publicly available information) on the workings of a hydrogen bomb. The Government sought to restrain the magazine from printing the story. A court preliminary injunction was later vacated after similar information was published in a newspaper."

The act's scope was broadened in 1981 to permit the Secretary of Energy to prohibit dissemination of certain unclassified information if dissemination could reasonably be expected to have a significant adverse effect on the health and safety of the public or the national defense and security by significantly increasing the likelihood of illegal weapons production or theft, diversion, or sabotage of nuclear materials, equipment, or facilities. Declassification alone may not release certain types of information from statutory control of its dissemination. 'g

The Export Administration Act and Arms Export Control Act. Both the Export Administration Act (50 U.S.C. App. 2401-2420) and the Arms Export Control Act (22 U.S.C. 2751-2794) provide authority to control the dissemination to foreign nationals of scientific and technical data related to items requiring export licenses according to the Export Administration Regulations (EAR) or the International Traffic in Arms Regulations (ITAR). The implementing regulations are administered by the Department of Commerce, which licenses items subject to EAR, and by the Department of State, which licenses items subject to ITAR. The export of communications and computer security products and technical data are controlled through EAR and ITAR. The Defense Department plays an advisory role regarding the application of these regulations to technical data.

The term "technical data" is defined broadly to restrict the domestic dissemination of scientific and technical information to foreigners, including the presentation of papers at open scientific meetings.[30] This broad definition of "export and the extent to which much scientific research can be (at least indirectly) related to items subject to controls have aroused much controversy during the past 7 years. The controversy pits the research and academic communities against the Departments of Commerce, State, and Defense.

Specific issues have included prepublication review clauses and other contract restraints on unclassified Government-sponsored university research, controls on foreign visitors, inquiries into and restrictions on foreign student activities (including access to supercomputer and advanced materials research), and DoD controls on the content of scientific communications at normally open professional meetings. An example of the latter was the meeting held by the Society of Photo-Optical Engineers in 1982, at which DoD forced the withdrawal of about 100 unclassified technical papers.[31]

[28] Harold C. Relyea: "National Security Controls and Scientific Information," CRS Issue Brief IB82083, June 17, 1986, p. 7.

[29] By contrast, uncontrolled dissemination of declassified documents–through NTIS, for example–has been criticized as being a continuing and important source of U.S. technology for the Soviet Union. See, for example: *Soviet Acquisition of Militarily Significant Western Technology: An Update*, DoD, 1985; and "Baldridge Claims U.S. Agencies Give Technology to Soviets," *Research and Development*, April 1985, p. 54.

[30] Relyea, op. cit., CRS IB82083, p. 8.

[31] See, for example: "Federal Restrictions on the Free Flow of Academic Information and Ideas, *Government Information Quarterly*, vol. 3, No. 1, 1986; Mitchel B. Wallerstein, "Scientific Communication and National Security in 1984," *Science*, vol. 224, pp. 460-466; Paul Mann, "Strictures on Non-Secret Data Concern Scientific Community," *Aviation Week and Space Technology, Nov. 19, 1984*, pp. 24-25; James K. Gordon, "Universities Resisting Potential Supercomputer Access Restrictions, *Aviation Week and Space Technology*, Aug. 26, 1985, pp. 59-62.

One of the outcomes of these controversies was the establishment of an ad hoc National Academy of Sciences Panel on Scientific Communication and National Security, chaired by Cornell University president-emeritus Dale Corson. The Corson panel report concluded that national policies of "security through secrecy" would ultimately weaken U.S. technological capabilities and recommended that contract controls be used for the (few) "gray" unclassified areas that could not reasonably be completely open.

The Invention Secrecy Act. The Invention Secrecy Act of 1951 (35 U.S.C. 181-188) provides that whenever the publication or disclosure by the grant of a patent on an invention—whether or not the Government has a property interest—might, in the opinion of the Secretary of Energy or the head of any designated defense agency (and the Department of Justice), be detrimental to national security, then that agency head can request the Commissioner of Patents and Trademarks to order that the invention be kept secret and withhold granting a patent. A patent secrecy order is issued for one year, but may be extended.

In addition to domestic patent secrecy orders, the Invention Secrecy Act provides that a license must be obtained from the Commissioner of Patents and Trademarks before filing any foreign patent application or registering any such design or model with a foreign patent office or agency for an invention made in the United States (35 U.S.C. 184).

Although the number of secrecy orders on cryptography patent inventions is small now, that was not always the case. According to a former director, NSA rescinded 62 of them in one year alone and sponsored 260 secrecy orders over a period of time.[32] It is not clear how much of a chilling effect prospective secrecy orders have on inventors.

The Defense Authorization Act of 1984. The Defense Authorization Act of 1984 provides authority to the Secretary of Defense to withhold from public disclosure certain technical data with military or space applications. The data must be in the possession or under the control of DoD and must fall within the scope of U.S. export control regulations (i.e., the data must be already subject to export controls) .33

[32]"Testimony of NSA Director, Admiral Bobby R. Inman, before the House Subcommittee on Government Information, Mar. 20, 1980. Also see "White Paper: Analysis of National Policy Options for Cryptography, " National Telecommunications and Information Administration, Department of Commerce, Oct. 29, 1980.

[33]Department of Defense Authorization Act, 1984. Public Law 98-94, Sept. 24, 1983, Sec. 1217, Authority to Withhold from Public Disclosure Certain Technical Data. 10 U.S.C. 140c.

Executive Branch Directives and Other Restrictions

As a compromise response to the controversy concerning restraints on the communication of scientific research and to the National Academy of Science's Corson Panel Report, President Ronald Reagan issued a directive on the transfer of scientific, technical, and engineering information on September 21, 1985. Known as National Security Decision Directive 189, (NSDD-189), the directive sought to minimize controls on fundamental research and to use classified procedures where controls are needed.

Specifically, NSDD-189 states:

> . . . to the maximum extent possible, the products of fundamental research remain unrestricted. It is also the policy of this Administration that, where the national security requires control, the mechanism for control of information generated during Federally funded fundamental research in science, technology, and engineering at colleges, universities, and laboratories is classification. . . . No restriction may be placed on the conduct or reporting of Federally funded fundamental research that has not received national security classification, except as provided in applicable U.S. statutes.

NSDD-189 made Federal agencies sponsoring research responsible for determining, before the award of a research contract or grant, whether classification is appropriate and for periodically reviewing grants and contracts for potential classification.

The directive did not quell all controversy, however, because it left "applicable U.S. statutes, such as the export control laws, available as an alternative method of controlling federally sponsored, unclassified research results. Since export controls on scientific information had been a cause of the original controversy, NSDD-189 thus failed to resolve the issue. [34]

[34]See: Relyea, op. cit., CRS IB82083, pp. 12-13; and "Reagan Issues Order on Science Secrecy: Will It Be Obeyed?" *Physics Today*, November 1985, pp. 55-58.

Meanwhile, the National Aeronautics and Space Administration (NASA) limits its distribution of some unclassified scientific and technical information, including that pertaining to dual-use technologies such as the space station, satellites, experimental aircraft, or transatmospheric vehicles. Such data can be restricted from dissemination to foreigners through export control laws, particularly through ITAR, or through other means (see below), if they have significant potential domestic benefit. Some NASA officials, however, feel a need for stronger protection against Free dom of Information Act requests from citizens of foreign countries. NASA officials try to screen such requests for unclassified reports listed in the RECON database, which contains abstracts and briefs from NASA technical reports. Foreign requesters are referred to the Department of State for licensing if the material is subject to ITAR.

NASA's charter calls for the agency to disseminate information in an "appropriate" manner. This can include "early domestic dissemination" of data that is subject to limited distribution, in which case the data is made available to U.S. industry with the proviso that it not be published or disseminated abroad for a period of time. In some cases, "appropriate" dissemination may be determined by consideration of U.S. economic competitiveness as well as by national security concerns.[35]

NASA does not make the services and documents in its technical utilization program available to foreign requesters or to their domestic U.S. representatives. For many years the NASA Scientific and Technical Information Facility has screened all requests for subscription to *NASA Tech Briefs*, technical support packages, and other documentation.[36] This practice, apparently motivated by concerns for national security and/or economic competitiveness and inferred from the export control laws, resulted in the NASA "No-No" list often being cited in the controversies surrounding National Telecommunications and Information Systems Security Policy Number 2 (NTISSP No. 2) 37 and the prospect of Government controls on commercial databases.

NTISSP No. 2 was formally adopted as national policy on October 29, 1986. It defines unclassified, but sensitive information to be used in accordance with the telecommunications and automated information system security policy set out in NSDD-145. NTISSP No. 2 extended Federal concerns for safeguarding information beyond national security interests to concerns for broader national interests as described above. Federal agency and department heads were directed to identify unclassified, but sensitive information that might warrant protection in telecommunications or information processing systems, to determine in coordination with the National Security Agency (NSA) the threats to and vulnerabilities of these systems, and to implement appropriate security measures consistent with Office of Management and Budget Circulars A-123 and A-130. (See ch. 5.)

NTISSP No. 2's broad definition of unclassified, but sensitive information and its implied extension of NSDD-145 into such a wide range of public and private sector information systems caused considerable controversy and outcry, as noted earlier, particularly because of implications for controls on scientific and financial information and commercial databases. NTISSP No. 2 was rescinded in March, 1987.

NSA does not have statutory authority to require prepublication review of independent, nongovernment research in cryptography. Nevertheless, the agency has attempted during the past decade to control publication and research funding in cryptography, efforts that

[35] OTA telephone interview with G. T. McCoy, NASA Office of the General Counsel, Patent Counsel Section, Mar. 31, 1987; comments from R. F. Kempf, Associate General Counsel for Intellectual Property Law, NASA, received May 8, 1987.

[36] Walter Heiland in NASA memo, "The So-called No-No List," dated Sept. 30, 1986.

370p. cit. National Policy on Protection of Sensitive, but Unclassified Information in Federal Government Telecommunications and Automated Information Systems, Oct. 29, 1986.

[38] "Making Waves: Poindexter Sails Into Scientific Databases," *Physics Today*, January 1987, pp. 51-52.

have caused controversy. In the mid- and late 1970s, NSA attempted to assume the responsibilities of the National Science Foundation for funding unclassified cryptographic research, including reviewing research proposals and results. [39]

NSA has also requested patent secrecy orders on applications for cryptographic equipment and algorithms under authority of the invention Secrecy Act. Controversy concerning two secrecy orders led NSA to request the American Council on Education (ACE) to form a study group on cryptography. The ACE group was assembled in 1980 and issued its report the next year. It recommended the establishment of a voluntary prepublication review arrangement between NSA and academic researchers. '()

As a result, NSA established a voluntary process for cryptographic manuscripts, with simultaneous review by NSA officials and professional journals, and with an appeals committee. Although the merits of such a process are still subject to some debate, some participants consider that it works in a reasonably satisfactory manner. According to Science magazine, about 200 papers had been submitted to NSA for review by 1984. According to NSA, of that number, nine papers were challenged. Six of these were modified and three withdrawn. [41]

[39] See ch. 4. See also Tom Ferguson, "Private Locks, Public Keys and State Secrets: New Problems in Guarding Information with Cryptography, " Center for Information Policy Research, Harvard University, April 1982, and "The Government's Classification of Private Ideas, " House Committee on Government Operations (op. cit.).

[40] "Report to the Public Cryptography Study Group, " *Academe*, vol. 67, December 1981.

[41] Mitchel B. Wallerstein, "Scientific Communications and National Security in 1984, " *Science*, vol. 224, pp. 460-466.

THE ENVIRONMENT FOR POLICY DEVELOPMENT

The Early Environment

Cryptography has long been the principal method for protecting the confidentiality of communications. Since World War I, and increasingly during the past four decades, the Federal Government has been the Nation's main source of expertise in the U.S. for developing cryptographic techniques. With rare exceptions, these developments, including cryptographic algorithms, have been kept secret, as has similar work in other nations.

Prior to the mid- 1970s, there were relatively few external complications to communications policies based exclusively on national security concerns. NSA, and DoD generally, had responsibility for communications security and the private sector had little interest in cryptographic technology. The Government could protect its interest by classifying R&D, controlling patent grants and exports, and monopolizing talent in the field. Any negative effect of this secrecy and controls on private sector activities, presumably, have been relatively minor, with the possible exception of restrictions on patents and exports of cryptographic equipment and technical data.

The Changing Environment and Federal Policies

During the past decade, a number of events have changed the external environment, changes that are still taking place. The first of these has to do with shifts in Federal policy and the second concerns the changing external environment for policymaking.

Federal policy took a sharp turn in the 1970s when a nondefense agency, NBS, became involved in cryptography for the first time. The result of NBS' efforts, which NSA assisted, was adoption of the Data Encryption Standard (DES) as a national standard for cryptog-

raphy, the inner workings of which were published in the open literature.

The change in policy direction from secrecy to openness appears to have signaled increasing interest in the defense and intelligence communities in finding ways to thwart the ability of the Soviet Union and others to gain access to unclassified, unprotected U.S. communications. The policy shift is widely known to have triggered debate within NSA as to the tradeoffs between potential gains in securing communications at the expense of losses to the agency's signals intelligence mission. Debates outside of the agency questioned whether NSA, in view of its signals intelligence mission, would permit a high quality cryptographic algorithm to be published in its entirety.

Then, in the late 1970s, heightened Federal concern for foreign interception of U.S. Government and private sector communications resulted in the issuance of Presidential Directive/National Security Council 24, as noted earlier. PD/NSC-24 called for raising public awareness of the vulnerability of communications systems to interception. Thus, cryptography, the central means for safeguarding communications that are easy to intercept, was destined to play a role in the security of nondefense communications.

As these Federal policies evolved, important changes were also taking place outside the Government as private sector interests and competence in cryptography and other safeguard technologies began to grow. These changes were stimulated by the almost simultaneous invention of DES and the public-key algorithm by researchers from industry and academia.(See ch. 4.) This was followed in the late 1970s and early 1980s by private sector users recognizing new applications for these technologies. The result was anew set of stakeholders with an interest in Federal policies in this area.(See ch. 5.) In addition, business interest in cryptography became international. These events contribute to an environment that contrasts sharply with the relatively tranquil one in which earlier U.S. policies were established.

The Current and Future Environment

The current external environment continues to evolve in a number of ways, some of which are an extrapolation of the past decade. For example:

- The private sector and civilian Government agencies are increasingly interested in improved safeguards for automated information systems, particularly for computer systems and for computer-communications networks. Computer safeguards are developing rapidly using a number of technologies, only a few of which are based on cryptography.
- Business applications for cryptography are still growing both in the United States and overseas.[42] Uses include improved confidentiality of data, message authentication and verification, and user identification. These new applications often take unpredictable forms, such as streamlining routine paper transactions in automobile manufacturing and reducing inventory costs in the grocery industry.
- There is an expanding, although by no means comprehensive, technical competence in the private sector to develop cryptographic-based and other safeguard technologies.

In this setting, defense policymaking has resulted in two recent changes. First, NSA sees its current role as the focal point for all computer and communications security for the Federal Government and private industry, including the protection of unclassified, but sensitive information.[4s]

Secondly, NSA changed the Federal Government's practice of openly publishing cryptographic algorithms. The agency announced in 1986 that it would not recertify DES-based products after January 1988. Previously endorsed DES products may continue to be used, in general, and DES also may continue to be

[42] "Richard I. Polis, "European Needs and Attitudes Toward Information Security, " unpublished paper prepared for the Fifteenth Annual Telecommunications Policy Research Conference, Airlie, VA, Sept. 27-30, 1987.

[43] NSA announcement, April 1986.

used for Government electronic fund transfers. [44]In place of DES, NSA announced that it would offer a family of NSA-designed and -certified algorithms embedded in tamper-proof modules to protect unclassified information.

[44]Letter from NSA to OTA from Michael C. Gidos, Chief, INFOSEC Policy, COMSEC Doctrine, and Liaison Staff, dated July 23, 1986.

Thus, the prior Federal Government policy of providing certified, published algorithms, developed as consensual standards under NBS stewardship, has in fact shifted to NSA-provialed, secret algorithms as a means of providing improved protection against the misuse of unclassified electronic information.

CURRENT CONGRESSIONAL INTEREST

The various interests, concerns, and policy trends described in this chapter provide a background for a set of policy issues reflected in proposed legislation and hearings on computer and communications security in Congress during 1986 and 1987. Issues and concerns that previously were spoken of privately now were said in public and for the record. The result may be a vehicle for resolving, at least in the short run, some of the conflicting interests and views of national security as they pertain to the security of computer and communications information.

The Computer Security Act of 1987 (HR 145) was introduced in the House of Representatives in 1987.[45] It would establish a Government-wide program to ensure the security of sensitive information in computer and communications systems. Specifically, the bill:

- assigns to NBS responsibility for assessing the vulnerability of the Federal Government computer and communications systems, and for developing appropriate security standards and guidelines, as well as providing technical assistance to other agencies;
- requires NBS to develop guidelines for use in training Federal personnel in computer security;
- defines unclassified, but sensitive information broadly to include information, "the loss, misuse, or unauthorized access to, or modification of, which could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under . . . the Privacy Act . . ."; and
- provides an advisor-y role for NSA to NBS concerning safeguard technology, but does not affect NSA's responsibilities for safeguarding classified information.

HR 145 establishes agency responsibilities for the development and standardization of safeguards to protect sensitive information against loss and unauthorized modification or disclosure, and to prevent computer-related fraud and misuse. As part of its role, NBS would develop standards and validation procedures for safeguards, provide liaison with other Government agencies and private organizations, and assist Federal agencies and the private sector in applying NBS-developed standards and guidelines. An advisory board would be established to assist NBS, which would include NSA representation.

Congressional hearings were conducted on HR 145 and NSDD 145 on February 25 and 26 and on March 17, 1987, by the Subcommittee on Legislation and National Security of the House Committee on Government Operations. Joint hearings were also held on February 26, 1987 by the Subcommittee on Science, Research, and Technology, and the Subcommittee on Transportation, Aviation, and Materials of the House Committee on Science, Space, and Technology.

The hearings were significant because they allowed representatives of important scientific,

[45]H. R. 145, The Computer Security Act of 1987, Jan. 6, 1987, and report 100-153, Parts 1 and 2, June 11, 1987.

professional, and trade groups to publicly express their concerns. Witnesses at the hearings commenting on their experiences or views on NSDD-145 were generally negative or apprehensive. Their comments tended to focus on three main points:

1. NSA's expanding role in civilian agency and private sector computer security;
2. the "disruptive," "counterproductive" effects of NSA's restrictions on U.S. banks' use of NSA-provided cryptographic algorithms; and
3. apprehension regarding potential DoD controls on unclassified information.

Many witnesses at these hearings were concerned that, under NSDD-145, the Government would restrict access to information in public libraries, engineering and scientific publications, and Government and commercial online databases. Challenges were raised as to the authority of the Government to withhold unclassified information from the public, the effect on First Amendment protections, and potential damage to the free flow of information in society and to the principle of open government [46]

In response, DoD officials assured the subcommittees that NSDD-145 would not extend the authority of DoD or NSA to control access to unclassified, but sensitive information, nor would it apply to information in the private sector or to Government information subject to release under the Freedom of Information Act. In commenting about the purposes of NSDD-145, these officials pointed out that the Government needs to prevent invasions of citizens' privacy, the obtaining of unfair advantage in business dealings, and avoidance of law enforcement efforts,[47] once again addressing the question of the scope of national security interests.

During the course of these hearings, the definition of unclassified, but sensitive information provided in NTISSP No. 2 was rescinded and the National Security Council initiated a review of NSDD-145 aimed at reducing or eliminating its operational role.[48] At about the same time, civilian agency participation in NTISSC was expanded.[49]

These current congressional activities are the latest attempt to grapple with the diverse issues surrounding information security policy, many of which are of long standing. Regardless of the outcome of HR 145, the fundamental issues–such as the separation of power, the role of the Government, and the boundaries between military and civilian agency responsibilities-will require reexamination to determine the appropriate balance of national interests.

[46] See, for example, testimony of the Information Industry Association, the Institute for Electrical and Electronic Engineers, the American Library Association, the Association of Research Libraries, the American Physics Society, David Kahn, and the American Civil Liberties Union.

[47] Op. cit., Latham testimony, Feb. 26, 1987.

[48] Letters from Frank Carlucci, Assistant to the President for National Security Affairs to Congressman Jack Brooks, Chairman, Committee on Government Operations, U.S. House of Representatives, Mar. 12 and 17, 1987; Letter from Howard H. Baker, Chief of Staff to the President, to Congressman Jack Brooks, Mar. 16, 1987.

[49] From material provided by NSA staff to OTA, Dec. 22, 1986.