

---

**Chapter 2**

# **Introduction**

# CONTENTS

	<i>Page</i>
Society's Changing Needs for Information Security . . . . .	13
Information Security and Government Policy . . . . .	15
Importance of Information Security Technology and Policies . . . . .	16
Business Interests in Information Security. . . . .	19
Conclusions . . . . .	19

# Introduction

---

On a day nearly 4,000 years ago, in a town called Menet Khufu bordering the thin ribbon of the Nile, a master scribe sketched out the hieroglyphics that told the story of his lord's life and in so doing he opened the recorded history of cryptology.

–David Kahn, *The Codebreakers: The Story of Secret Writing*

Information technology is revolutionizing society as profoundly as mechanical technology did in creating the industrial revolution. As a result, we are increasingly dependent for society's everyday functioning on electronic ways to gather, store, manipulate, retrieve, transmit, and use information. By all accounts, the importance of automated information systems and the communications systems that link them will continue to increase and transform the way we conduct our government, business, scientific, and even personal affairs.

This increasing dependence on information technology is creating a need to improve the confidentiality and integrity of electronic information, i.e., its security, so that computer and communications systems are less vulner-

able to intentional and accidental error or misuse. This will allow us to use the new systems with confidence in a widening range of applications, such as electronic contract negotiations, with assurance that private, proprietary, or intellectual information entrusted to them will be properly protected.

Progress is being made in developing techniques for satisfying these needs. However, both the pace and direction of this progress will be affected by two factors:

- the traditional use of Federal information security policy, often as a means of implementing national security goals; and
- the need to accommodate the variety of national interests that are affected by Federal policy on information security.

To put the topic in perspective, just as information security is a small, but vital part of the larger framework of information technology, Federal policy on information security is a reflection of broad national interests, rather than that of national security alone.

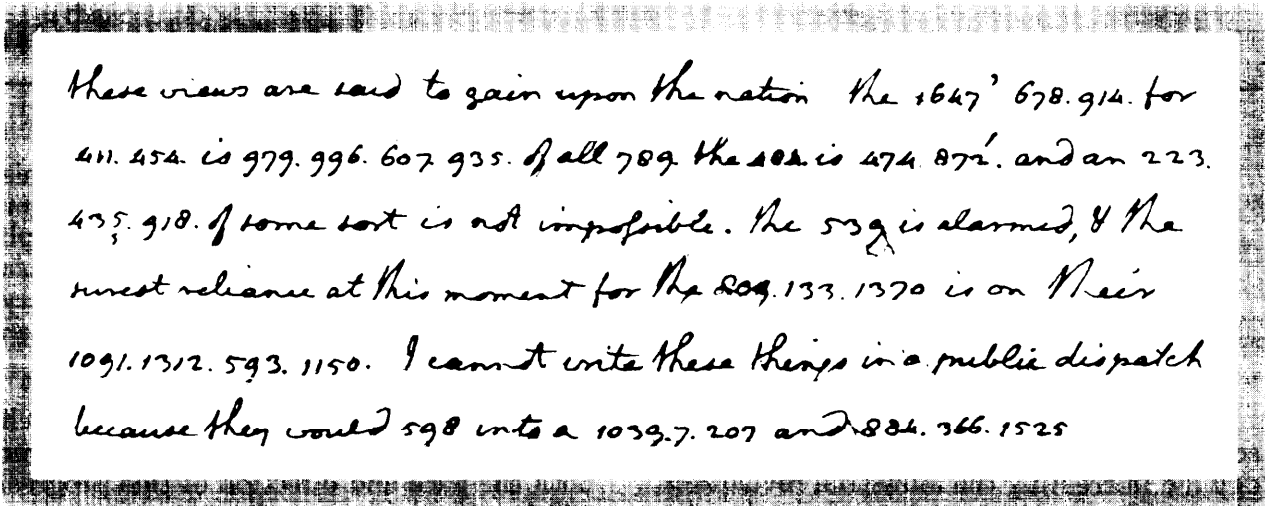
## SOCIETY'S CHANGING NEEDS FOR INFORMATION SECURITY

The need for information security is not new. It dates back hundreds, even thousands, of years. Methods for conveying confidential messages were used in ancient Greece and much of the Western world by kings, generals, diplomats, and lovers. Today, the governments of most developed nations make extensive use of encoding techniques to keep their sensitive electronic communications secret.

Technology itself has long played a leading role in causing certain attributes of information security to become highlighted. The introduction of the telegraph brought concern about eavesdropping. Inexpensive sound and video recording capabilities raised concerns

about unauthorized reproduction. And the proliferation of electronic storage quickly brought questions of how to prevent misuse of electronic data. Indeed, most of the attributes of information that are of concern today —confidentiality, accuracy, accountability—have long existed. Technological advances have not only modified their importance but have also introduced fundamentally new issues.

Today's technology provides new capabilities that raise both familiar and new concerns for security. High on the list of current concerns are the need for controls on capabilities for accessing, altering, and duplicating electronic data, and the ease of retrievability and



these views are said to gain upon the nation the 1647' 678.914. for  
 411. 454. is 979. 996. 607 935. of all 789. the sea is 474. 872. and an 223.  
 435. 918. of some sort is not impossible. the 539 is alarmed, & the  
 surest reliance at this moment for the 209. 133. 1370 is on their  
 1091. 1312. 593. 1150. I cannot write these things in a public dispatch  
 because they would get into a 1039. 7. 207 and 884. 366. 1525

Segment of original letter (top) and translation (bottom) from Thomas Jefferson to James Madison, August 2, 1787. Reproduced from *The Papers of James Madison*, vol. 10, 1787-1788, pp. 124-126. Library of Congress.

These views are said to gain upon the nation. The *kings passion* for drink is *divesting* him of all respect. The *queen* is *detested* and an *explosion* of some sort is not impossible. The *ministry* is alarmed, & the surest reliance at this moment for the *public peace* is on their *two hundred thousand men*. I cannot write these things in a public dispatch because they would get into a newspaper and come back here.

searchability of databases. Still other concerns include ensuring the accuracy of messages and verifying their origin, and providing means for auditing or reconstructing transactions. These concerns have arisen both in Government agencies and in businesses worldwide because traditional physical security measures are limited in their ability to prevent misuse of information in today's automated world.

In addition, as information technology increasingly substitutes for paper-based systems, it is important to retain familiar capabilities of the older technology. In fact, many of the developments in security are attempts to imbue in modern information systems parallels to the more familiar safeguards and procedures of paper-based and face-to-face forms of business transactions that we have become accustomed to using—as discussed later.

Some security techniques are adaptations of earlier ones, while others are genuine innovations. Modern equivalents of such traditional security tools as passwords, notary public

“seals, codebooks, physical identification, separation of authority, and auditable book-keeping procedures are all being used or considered today, separately or in combination, to contain misuse of electronic information. Prominent among the recent innovations are public-key cryptography, and the “zero knowledge” proof. The former may be used to establish private communications between previously unacquainted parties, as well as to provide the electronic equivalent of a personal signature. The latter can be used to demonstrate that a person knows a piece of information without revealing the information in the process. For example, it could be used to demonstrate knowledge of a solution to a “hard problem” without revealing anything about the specific solution method. Each of these innovations have broad implications for new applications of information technology.

Such encryption-based safeguards provide a basis for today's sophisticated information security technology and an expanding range

of commercial applications. Banks are beginning to use these technologies to safeguard electronic fund transfers. Similarly, some companies are beginning to use them to protect the confidentiality of electronic mail and to replace paper-based business transactions with

less expensive electronic equivalents. Expanding these capabilities to include proof of message receipt and acceptance, and protection of the anonymity of those taking part in transactions, is likely to require further innovation.

## INFORMATION SECURITY AND GOVERNMENT POLICY

Federal policy for the security of electronic information was, until recently, an obscure topic having little public interest. In the first place, virtually all such policy was related to the secrecy of military, intelligence, and diplomatic information. Second, the authority and expertise for keeping information secure rested with defense and intelligence agencies that normally do not engage in open policymaking. Moreover, except for defense contractors, Federal policies had little effect on the public or on private businesses.

The Government's national security focus created an incentive to control the proliferation abroad of communications safeguard products and, in fact, to control the technology itself. The purpose was to deny foreign adversaries access to valuable U.S. technology and to protect the viability of U.S. foreign intelligence operations.

During the 1970s, the National Bureau of Standards (NBS) began to develop computer security standards for use by Government agencies based on its authorities stemming from the Brooks Act of 1965. In 1977, with technical assistance from the National Security Agency (NSA), NBS adopted the Data Encryption Standard (DES) as the national standard for cryptography. For the first time, a published cryptographic standard became available for civilian agencies, and it quickly was adopted by business users and the American National Standards Institute as the basis for many industry standards. NBS also began to validate commercial products implementing DES, thereby increasing users' confidence in the products' conformance with the

Federal standard. As a consequence, DES is gradually becoming used for many applications.

Interest in information security is now worldwide and an active area of research and development in western European countries and Japan. DES has been considered as an international standard during recent years in forums composed of representatives from international businesses and governments (see ch. 5).

The proliferation of information technology has made more sensitive data accessible to more users, thereby creating another form of new vulnerability to misuse. In order to limit potential damage to U.S. interests, particularly from foreign intelligence agencies, the executive branch has sought to control access to unclassified information that it deemed sensitive. Although the definition of such information has been open to considerable debate that is still unresolved, it may include proprietary information filed with defense agencies and the Environmental Protection Agency, economic data collected by the Commerce and Treasury Departments, and personal data kept by the Department of Health and Human Services.

Policy directives issued by the executive branch in 1984 and 1986, and ensuing congressional hearings in early 1987, have significantly increased public concern over Federal information security policy. The expanding pattern of defense-intelligence interests as a central focus in the formulation of policy is seen as competing with other major national interests and has become the subject of public debate. The focus of the debate has been on the potential impact of these policies on some fundamental tenets of American government: the separation

of and appropriate balance between defense and civilian authority, constitutional rights, open science, and Government controls on public access to information. The debate also raises the question of how to resolve conflicts involving the boundary between the authorities of the legislative and executive branches in making policy when national security is a consideration. On a more practical level, there are also

serious misgivings about the applicability of the security approach taken by the Department of Defense (DoD) to the needs of the private sector.

At the same time that these Federal policies and their effects have been unfolding, trends are visible that may significantly influence commerce and other private sector interests.

## IMPORTANCE OF INFORMATION SECURITY TECHNOLOGY AND POLICIES

Interest in information security technology now clearly extends beyond the Federal Government to the private sector as well. Its importance to business and society cannot be gauged adequately by the dollar amount of sales of products, but by the range of applications that the technology makes possible.

Safeguard technology is likely to become a mainstay for facilitating tomorrow's automated world of finance, commerce, and law, much as automated message authentication and verification are now becoming essential for the banking industry worldwide. These technologies are used to authorize transactions, authenticate users, verify the correctness of messages and documents, certify that legitimate transactions have occurred and identify the participants, and protect individual and corporate privacy.

Such applications are likely to be used to establish a legally valid electronic equivalent of the centuries-old, paper-based systems for authorizing access to information, identifying parties to agreements, authenticating letters and contracts, ensuring privacy, and certifying value. In this sense, they will replace such traditional safeguards as letters of introduction, signatures, and seals, and assume an importance difficult to foresee from the limited applications of today.

Both Government and industry are interested in improving the security of information they own or are entrusted with. Two major

trends reflect these interests and are bringing attention to the direction of Federal policy. One concerns the Federal Government's need to keep an increasing amount of unclassified information confidential while, at the same time, gathering intelligence from other countries. The question of what information ought to be kept confidential, or have access to it controlled, is not well defined, but subject to judgments concerning potential damage to the Nation's security; examples of such information might include corporate proprietary data that could benefit foreign competitors or data useful to terrorists. The other trend is the evolving and growing need of the private sector to safeguard certain of its information and information resources from theft, destruction, or other misuse.

Federal policy has been formulated both by the executive and legislative branches, sometimes with similar purposes. Policy in information security has often been set by the President, based on national defense needs. This has invariably led to a major role for the DoD. Legislation, on the other hand, has also been used to establish policy for information security. The latter has often been based on other national interests, such as the privacy of telephone communications and of data in Government computer systems. Such laws typically have involved civilian agencies in their implementation.

Society's needs and the new demands stimulated by technology are causing these sepa-

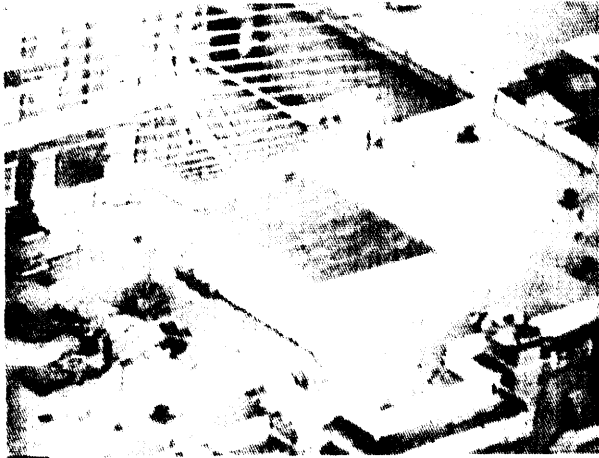


Photo credit Courtesy of NBC News Video Archive

Roof of Soviet embassy in Washington D.C.  
showing antennas

rate policy paths to converge. With this convergence, major stresses are becoming visible in the balancing of competing national interests and with the process by which policy is developed.

The focus of information security policy on the military, intelligence, and diplomatic interests of Government has particular significance for the issues of today for two interrelated reasons. First, responsibility for protecting the security of Government electronic information is consolidated within the defense and intelligence communities, where NSA has been given the lead responsibility. The second concerns the broadening scope of executive branch actions taken for reasons of national security. There is a tendency for this concern to include unclassified, but sensitive information.

NSA was created in 1952 as an agency of DoD by secret Executive Order. For decades its existence was not made public, and the only extensive public description of its operations were provided in the book, *The Puzzle Palace*, which the agency tried to prevent from being published.<sup>1</sup> NSA has been the subject of considerable controversy during the past decade due to its secret operations.<sup>2</sup>

<sup>1</sup>James Bamford, *The Puzzle Palace* (New York, NY: Penguin Books, 1983).

<sup>2</sup>Ibid.

NSA functions are a consolidation of missions previously performed by each of the military departments. One of its two main missions is foreign signals intelligence, i.e., gathering information principally by intercepting and decoding electronic communications. It also protects U.S. military and diplomatic communications by enciphering them or making them less accessible to interception by the intelligence agencies of other countries. Such work is classified. NSA's work in developing encryption techniques, however, has made it the undisputed technical leader in the United States. More recently, the agency has widened its scope to include computer security.

Some of these Government efforts to reduce vulnerabilities from unauthorized access to communications systems are also creating tensions with other defense and intelligence interests. To the extent that methods to reduce unauthorized access to these systems enter the public domain, they can be used by other countries, thereby damaging NSA's ability to gather intelligence.

Since the 1970s, DoD has become increasingly concerned about the vulnerability of U.S. communications to foreign intelligence activities. As a result, NSA has launched several programs to better safeguard the Government electronic communications. NSA has also encouraged domestic common carriers to provide tariffed "confidential" communications services for customers and has briefed dozens of U.S. companies on the vulnerability of communications systems to interception.

Second, where "national security" has generally been used to control classified military and certain diplomatic electronic information, executive branch directives of 1984 and 1986 extend this rationale to encompass unclassified information considered to be sensitive.

A current debate concerns the appropriate agency for Federal leadership for developing security standards for civilian computer systems—NSA or the Department of Commerce's NBS. However, the core issue is more basic. It goes to the question of whether or not a defense agency should control matters that are

central to civilian interests, such as commerce and the free market, constitutional rights, and principles of open science. It also involves questions about executive branch authority under the Constitution to set policy based on national security. Yet a third dimension involves society's evolving needs for information security and the appropriate Federal role in accommodating those needs.

The event that triggered the current examination of Federal policy was the National Security Decision Directive 145 (NSDD-145), dated September 17, 1984. That executive branch directive established as Federal policy the safeguarding of unclassified, but sensitive information in communications and computer systems that could otherwise be accessed by foreign intelligence services and result in "serious damage to the U.S. and its national security interests."

NSDD-145 also created an interagency management structure to implement the policy. It gave leading roles to the National Security Council, DoD, and NSA. These roles include defining what information to protect, deciding on the appropriate technology for safeguarding unclassified information, developing technical standards, and assisting civilian agencies in determining the vulnerabilities of systems to misuse.

NSDD-145 raised numerous questions from critics in other Government agencies as well as from civilian sources, some of which relate to the broader issues mentioned above. They include concern for:

- intermingling defense and civilian matters;
- public access to Government information;
- the legislated responsibility of NBS to develop computer standards for the Federal Government under the Brooks Act of 1965, as amended;
- private sector development and use of safeguard technology; and
- expanding the responsibilities of NSA in civilian matters, particularly in light of the conflict of interest between its intelligence mission and commercial needs, and its lack of direct public accountability.

The level of public concern was elevated further with the release by the National Security Council in October 1986 of a policy statement defining what information is sensitive and therefore possibly in need of safeguarding.<sup>3</sup> The release coincided with well-publicized Government activities aimed at identifying and possibly restricting access by selected foreign governments to unclassified, but sensitive data in Government and commercial automated information systems. As a result, the issue of Government restrictions on public access to unclassified information, whether or not in Government systems, has become a public concern. The statement, though rescinded in early 1987, caused public alarm that illustrated the extent of sensitivities among diverse organizations concerning controls on unclassified information.

Perhaps the major effect of these executive branch policies to date has been to encourage an examination by Congress of the effects of such defense-oriented policies on civilian matters. Legislation has been proposed to reestablish civilian control over the security of unclassified information systems. In the short term, many of the currently prominent issues related to information security policy are likely to be addressed by congressional debate over the proposed legislation, including the respective roles of NBS and NSA in setting standards and the measures to be taken, if any, to control access to unclassified information.

For the longer term, however, the vulnerabilities to misuse of information systems will depend on the development and widespread use of technical, administrative, and related safeguards. The availability of high-quality information safeguards worldwide, especially cryptographic-based systems, on the other hand, will make intelligence gathering more difficult for the United States.

<sup>3</sup>National Policy on Protection of Sensitive, but Unclassified Information in Federal Government Telecommunications and Automated Information Systems, National Security Council, Oct. 29, 1986.



## BUSINESS INTERESTS IN INFORMATION SECURITY

The question of the extent to which information systems should be protected depends on the various perceptions of threats to those systems. Simply put, U.S. defense and intelligence agencies are concerned about unauthorized access to commercial communications and computer systems by the intelligence organizations of foreign countries, particularly the Soviet Union. However, U.S. businesses or civilian agencies generally do not consider their main risk to be from such sophisticated adversaries.

The range of threats to business information systems is not as broad as that faced by defense and intelligence agencies. Business concerns for misuses are mainly by insiders, competitors, and, to a limited extent, hackers.

Companies that safeguard their communications seem either to have business interests at risk (e.g., banking and oil exploration firms concerned about unauthorized interception) or are required by the Government to use prescribed safeguards (e.g., Federal Reserve banks and defense contractors). A number of businesses are finding additional reasons to provide some safeguards for information in computers and communications systems. These reasons include prudent management of resources and methods of improving efficiency, as well as preventing the loss of proprietary information or theft of funds. Private businesses, in addition, often are more concerned with information integrity rather than confidentiality.

For their part, businesses need safeguards that do not unduly slow down or otherwise im-

pair normal business operations; that is, in order to be useful, security measures must be practical and efficient. U.S. firms engaged *in* international commerce and banking, to be able to use these systems, also must be able to export them to their subsidiaries in other countries.

Concern for cost is an area in which contrasts between defense and intelligence agencies and business interests are even more apparent. Private businesses must remain profitable and competitive, and, therefore, they resist safeguards unless they are cost-effective. Defense and intelligence agencies, because of their missions, are more tolerant of higher costs or of operational impediments that might result from adopting security measures. One of their most important goals is to prevent valuable information from falling into the wrong hands, even if significant trade-offs are involved.

Nevertheless, there are many similarities between the various defense and nondefense, as well as between Government and private sector, requirements for information security, although their requirements vary widely. Both need to control access to databases, restrict unauthorized activities, provide audit capabilities, safeguard sensitive data and transactions, and, generally, maintain the integrity of data and continuity of service. Thus, Federal policies that affect the longstanding NBS and NSA roles in developing technology to safeguard information systems will also affect private sector security programs.

## CONCLUSIONS

The need for information security has existed for a long time. The particular attributes of security perceived to be important tend to change emphasis with time and technology, often in ways that are difficult to predict with confidence. Society's ability to satisfy its

changing needs for improved security depends on its ability to adapt existing technologies and techniques as well as to innovate (see ch. 4). Government policy can be an important determinant of how, when, and by whom these needs are satisfied.

These conclusions imply that policies predicated solely on solving current security problems are not likely to endure because needs for information security are not static. Further, those based on controlling or restricting private sector actions are likely to damage other societal needs. In other words, flexibility and balance are important objectives of any policy intended to accommodate a wide range of users' needs on a continuing basis. Moreover, it seems apparent that U.S. policies that cannot effectively be enforced internationally risk being overcome by events in other countries.

Further, information security policy has a significance that is colored by different interests. One view sees its significance as relating mainly to the potential for foreign government intelligence via U.S. communications and computer databases and other threats to national security. From a different viewpoint, however, the significance of information security involves even more diverse interests. These include basic democratic principles and civil liberties, as well as commercial business interests.

In addition to these interests, each of which has its advocates, there is at least one other that has no clear advocate—the evolving needs of society for information security. Society's needs for information security has a long his-

tory that is continually evolving. Federal policy also has an influence on advances in the technology underlying information security applications, especially when the technology itself is controlled for national security purposes.

Regardless of the viewpoint taken, information technology poses a challenge to Government, industry, and society. Modern information systems and the data within them are vulnerable—they can easily be misused. The challenge is to find ways to reduce the risks to acceptable levels while preserving traditional democratic values and remaining flexible to accommodate diverse and changing needs.

The remainder of this report examines some of the technological foundations for information security and the main policy issues that are now evolving. In order to focus attention on the issues facing Congress, many topics have been treated in a limited way. The report is not about potential disruptions to or recovery from disasters, for example, nor is it about physical security or safeguarding classified information or constitutional rights. Its purpose, instead, is to describe the conflicting national interests that are shaping U.S. information security policies, the special role of cryptography and NSA's intelligence mission, and the potential courses of action.