Chapter 1

Executive Summary

CONTENTS

Chapter 1

Executive Summary

As society becomes more dependent on computer and communications systems for the conduct of business, government, and personal affairs, it becomes more reliant on the confidentiality and integrity of the information these systems process. Information security has become especially important for applications where accuracy, authentication, or secrecy are essential.

Today's needs for information security are part of a centuries' long continuum that shifts in emphasis with changing technology and societal values. Modern electronic information systems are expanding the need for both familiar and new forms of information security.

> Today's needs for information security are a part of a centuries' long continuum.

Developing adequate information security technology is a challenging task. This task is further complicated since some of these evolving needs can only be satisfied with technology that must itself be kept secret, according to Department of Defense sources, because revealing it could be damaging to U.S. intelligence operations.[1] This situation raises the practical question of whether safeguards designed for use by defense and intelligence agencies can meet the needs of commercial users without jeopardizing U.S. intelligence objectives, i.e., whether the National Security Agency (NSA) can reconcile its traditional secret posture with the openness needed to solve nondefense problems. It also raises the broader issues of the appropriate role of defense and intelligence agencies in civilian matters, and how openness and free market forces can coexist with secret operations and controls on sensitive information.

Policy for information security, long dominated by national security concerns, is now being reexamined because of its broadening effects on nondefense interests. At the center of the current controversy is the appropriate role of the Federal Government in information security. The immediate policy questions focus on whether NSA, primarily an intelligence agency, or the National Bureau of Standards (NBS), a civilian agency, should be responsible for developing information security for nondefense applications. A fundamental issue is how to resolve conflicts involving the boundary between the authority of the legislative and executive branches to make policy when national security is a consideration; a topic with implications extending well beyond the narrow confines of information security policy.

A separate, but related dimension to policymaking involves recent efforts to provide additional Government controls on unclassified information in computer databases, some Federal, some commercial. Proponents of greater Government controls argue that these databases make information so readily available to foreign governments, competitors, and those having criminal intent, that uncontrolled access to them is a threat to national security.

Congress is responding to these issues by examining alternative Federal roles in information security. Each of the three basic options for providing leadership-through NSA, NBS, or greater reliance on the private sector—has its own particular drawbacks and none is likely to completely satisfy all national objectives.

There are a number of national interests to be accommodated by policy makers. An optimum outcome would maximize the ability of free market forces to develop and apply technology to meet users' diverse and unfolding needs for information safeguards, while avoiding unnecessary restrictions on trade, innovation, and the free flow of information as well as compromises to the Nation's security.

[1] The terms intelligence and intelligence operations are used throughout this assessment to refer to signals intelligence.

THE NEED FOR INFORMATION SECURITY

The need for information security has existed for thousands of years, but the advent of electronic information systems—telegraph and telephone, sound and image recording, and computers and databases—has reemphasized the need for traditional safeguards and created a need for new ones. Early concerns tended to focus on controlling access to information and protecting its confidentiality.

Modern computer and communications systems are being used in ways that often require those using them to authenticate the accuracy of data, verify the identity of senders and receivers, reconstruct the details of transactions, and control access to sensitive or private data. As the use of these systems increases, the vulnerabilities, threats, and risks of misuse have become clearer, and information security has become a prominent issue for many Government agencies and private users.

Electronic information systems—telegraph and telephone, sound and image recording, computers and databases—reemphasize the need for traditional safeguards and create needs for new ones.

The computer and communications technologies on which these information systems are built, however, were not developed originally with information security in mind. They were designed for efficient and reliable service in the presence of accidental error, rather than intentional misuse, and little attention was given to protecting confidentiality. As one result, the public communications network has always been vulnerable to exploitation by those with appropriate resources (see below).

Information security was not a key factor in the design of most computer and communications systems. As a result, some forms of unauthorized access, such as wiretaps, intercepting mobile telephone conversations, or logging into computers with easily guessed passwords, can be achieved with limited resources.

Technology can increase or decrease the vulnerability of communications to misuse. Microwave radio and cellular telephones have both increased vulnerability; optical fibers have decreased it. Still greater changes may be ahead as digital communications come into wider use.

Increases in computing power and decentralization of computing functions have increased the vulnerability of computer and communications systems to unauthorized use. Two types of misuse should be distinguished: misuse by those not authorized to use or access systems and misuse by authorized users. For many public and private organizations, the latter problem is of greater concern.

The level of effort, expense, and technical sophistication needed to gain unauthorized access to computer or communications systems, even when the system being attacked employs no special safeguards, can vary widely. Some forms of covert access, such as wiretaps, intercepting mobile telephone conversations, or logging into computers with easily guessed passwords, can be achieved with very limited resources. Others, such as those intended for targeted and consistently successful unauthorized access, can require greater resources due to inherent barriers in the design of these systems. Systems protected by appropriate safeguards can deny access even to dedicated foreign intelligence agencies.

Users of computer and communications systems have widely different perceptions of the threats against which protection is needed.

Some users protect their systems only against unintentional error or amateur computer hackers. Others guard against misuse by their own employees, outsiders, or the sophisticated intelligence agencies of foreign countries.

> Many businesses are concerned with the integrity of certain of their computer information, but not greatly concerned with threats to the confidentiality of their domestic communications.

There are few publicized cases of communications interception and most of these deal with the interception of government communications by foreign intelligence agencies. Not surprisingly, most commercial and private users, under ordinary circumstances, are not greatly concerned about their communications, particularly within the United States, being intercepted by foreign governments or others. Indeed, many businesses are concerned primarily with the integrity of certain of their business information and, in other cases, with the confidentiality of their sensitive information.

Early computer systems were designed to be used by trained operators in reasonably controlled work environments; therefore, only local access to the systems was of concern. Today's systems, in contrast, are often designed to be used by, almost literally, anyone from anywhere. With this ease of access to computers, new problems have emerged, both from hackers and other unauthorized users, and from employees authorized to use the systems. Available data suggest that the damage done by computer hackers to poorly safeguarded systems is less severe than originally thought, and that actual and potential misuse from employees who are authorized to use the systems is far more significant.

On the other hand, NSA is concerned with foreign intelligence gathering, a concern that has motivated it to launch programs to improve the security of nondefense computer and communications systems.

Thus, even though virtually all users have concern for some combination of confidentiality, integrity, and continuity of service, the business community and the Government agencies that deal with it often have a very different outlook and need than defense and intelligence agencies when it comes to safeguarding information in computer and communications systems. This difference is one reason why some of the business community has been reluctant to accept safeguard technologies based on NSA's assessment of needs or that are tightly controlled by NSA.

Safeguard Technology

> Important techniques are emerging to improve the security of information in these systems including technical means to verify the identities of the senders of messages, authenticate their accuracy, and ensure confidentiality.

The private sector is developing a number of ways to safeguard information in computer and communications systems. These include technologies to encrypt data to make it confidential and to control access to computer systems (such as with personal identification techniques), as well as to audit system activity and other administrative procedures. In many cases, commercial safeguards for these systems are still evolving, as are users' understanding of their needs for them.

The use of information safeguards, *properly* applied, can vastly increase the level of resources required for potential adversaries to successfully gain access to protected systems. Some safeguards require two or more people, Innovation is especially important for the evolution of new applications of information security.

often trusted employees, to collude in order to gain unauthorized access, while others leave audit trails to identify how the system was misused and by whom. But technical safeguards alone cannot protect information systems completely; effective management policies and administrative procedures are also needed.

Safeguard products are based both on adaptations of existing technology and on innovations. Some of the approaches to controlling access, for example, rely on the use of passwords or hand-geometry measurements. Techniques for authenticating messages include those that make use of newly developed mathematical techniques called public-key cryptography and electronic procedures for providing "digital signatures" to verify the identity of the sender of a message.

As is already becoming clear with cryptography, innovation is especially important for the evolution of new applications of information security. The capabilities now evolving will allow advances in the way many electronic transactions take place, from digital signatures and legally enforceable electronic contracts to improved individual and corporate accountability and assured confidentiality of transactions. The potential of cryptography and related mathematical techniques for transforming the ways in which automated transactions are accomplished has only begun to be explored for applications in finance, commerce, law, and government.

Some new safeguard techniques have only begun to be explored, but show promise for broad applications in commerce and society.

Users' Needs and Actions

Commercial and other users want greater information security to reduce fraud, embezzlement, and errors; cut the costs of operations; and protect proprietary and private data. Users have begun to incorporate information safeguards in a gradually expanding range of applications. For example, information security is being applied in the banking industry to reduce errors and opportunities for fraud, and in other industries as part of an increasing reliance on electronic, rather than paper-based, transactions. These electronic transactions allow businesses to simplify paper work and reduce inventory costs,

Although there are significant differences in the needs for information security even among users within the same industry, civilian users often focus on data integrity. They also tend to be especially sensitive to the importance of the ease of use and cost-effectiveness of safeguards. Many defense needs, too, resemble those of civilian users, but in addition, some defense functions, especially intelligence activities, have a primary need for confidentiality. These latter needs must be ensured, even if they entail higher cost or lowered ease of use.

Business users have tended to consolidate their requirements for common information safeguards through voluntary participation in the activities of U.S. and international organizations that develop open public standards. In contrast, NSA sets its own standards in a process that is sometimes open to the public (as is typical for computer security) and sometimes not (as is typical for communications security). These and other differences raise the question of whether information safeguards designed by and for the defense and intelligence agencies are well suited to the needs of commercial and other users.

THE ROLE OF THE FEDERAL GOVERNMENT

The Federal Government has played an active role in the development of information safeguards. NSA was established to unify U.S. signals intelligence operations against foreign communications and to protect U.S. military, intelligence, and diplomatic communications against foreign government intelligence gathering efforts. As NSA's concerns expanded to include computer security, the agency has begun to provide technological leadership for civilian uses of information safeguards, presumably in ways that minimize the impact on its foreign intelligence operations.

> Federal policy for information security has long been dominated by national security interests and controlled by DoD and NSA.

In addition, the National Bureau of Standards has played a central role in setting information security standards for civilian Government agencies and certifying commercial products. NBS's role stems from the Brooks Act of 1965, which authorized it to set standards for computers used by Government agencies.

> A civilian agency, NBS, has become active in the development of computer security standards since the mid-1970s. Recent policy directives, however, have shifted control back to DoD and NSA, raising questions of the boundary between civilian and military authorities.

> its activities in providing standards and specifications, certifying equipment, and developing secret cryptographic algorithms, have made the Government influential in the decisions of some industries about their use of information safeguards.

NBS, with the active technical support of NSA, spearheaded the development of a national standard for cryptography, the Data Encryption Standard (DES). DES, which was adopted by NBS in 1977, has become the basis for many private cryptographic standards. It is also the standard in use by other civilian Government agencies. In addition, both NBS and NSA have facilitated the entry of cryptographic-based safeguards into the market by certifying and endorsing commercial products and developing guidelines for their use.

In the mid-1980s, however, changing Government policies provided *new* direction for the Federal role in, and leadership for, information security. National Security Decision Directive 145 (NSDD-145), issued in 1984, expanded Federal concerns to include "safeguarding systems which process or communicate sensitive information from hostile exploitation, established a high-level interagency group to implement the new policy, and assigned key responsibilities to the Department of Defense and NSA,

One result of NSDD-145 was to authorize NSA to develop information safeguards for Government agencies to protect unclassified information. In effect, this meant that responsibility for certifying DES as a national standard and other safeguard technologies was transferred from NBS to NSA. In a major shift in policy, NSA announced in 1986 that it would no longer certify DES-based products for Gov-

> There has been controversy about DoD restrictions on the export of cryptographic equipment embodying classified technology.

There are significant differences in users' needs for information security even among users within the same industry, which raises the question of whether information safeguards designed by and for defense and intelligence agencies are well suited to the needs of commercial and other users.

ernment use beginning in 1988. Instead, NSA said it will supply its own, secret cryptographic designs for use by U.S. companies and civilian Government agencies—a move that has raised some industry concerns because it might result in restrictions on the use of equipment embodying these designs and it might also allow NSA itself to eavesdrop on corporate communications.

This shift of responsibilities from NBS to NSA raised several other questions. One involves the efficacy of NSA-developed standards and guidelines for users outside the national security community. Another question concerns the scope of NSA's activities in light of NBS's legislated responsibilities under the Brooks Act.

In a later directive[2] intended to implement NSDD-145, the National Security Council placed new controls on what it called unclassified, but sensitive information in various Government information systems and commercial databases. These efforts raised such a protest from scientific and civil liberties organizations and the business community that the directive was rescinded during the course of congressional hearings in 1987 and NSDD-145 itself was put under review.

In the current reexamination of policy on information security, the immediate policy question is whether NSA or NBS should be responsible for nondefense applications.

The expanding sphere of national security concerns embedded in information security policy is now seen as competing with other national interests and affecting basic principles such as the appropriate balance between defense and civilian authority and public access to information.

These changes in Federal policies on information security indicate an expanding sphere of "national security" concerns—a concept whose definition is subject to interpretation and change. The changes point out clearly that Federal policy for information security, until recently a topic of little concern beyond the Government's defense and intelligence communities, now has significant impact on much broader areas of national interest, including commerce, innovation, free flow of information, and civil liberties. They also indicate that tensions are likely to recur as the use of automated information systems continues to expand.

Longstanding fundamental issues include how to resolve conflicts involving the boundary between the authority of the legislative and executive branches when national security is a consideration and the process by which these policies are developed.

‘National Policy on Protection of Sensitive, but Unclassified Information in Federal Government Telecommunications and Automated Information Systems, National Security Council, Oct. 29, 1986.

POLICY ALTERNATIVES

Federal policy for the security of information in computer and communications systems seeks to achieve a number of objectives ranging from protecting national security to fostering development of private sector competence to meet its own needs. Policy might also seek to establish a structure within the Government that can provide leadership and standards both for defense and intelligence purposes and for the business community, Although there are often strong differences of opinion on the merits of specific Federal policies, there seems to be broad agreement on the types of goals that such policies might aim to achieve. Some of these goals are to:

- foster the ability of the private sector to meet the evolving needs of businesses and civilian agencies for information safeguards;
- minimize risks to intelligence capabilities resulting from independent, private sector developments;
- clarify the roles of Federal agencies concerning safeguard technology, particularly those of NSA and NBS;
- promote competition, innovation, and trade;
- separate, where practical, defense and intelligence agencies' missions from those of the private sector and civilian agencies; and,
- minimize or reduce the tensions between Federal policies and private sector activities.

The basic alternatives for policy center around the relative roles of NBS, NSA, and the private sector in providing leadership in the technological development and use of safeguards for unclassified electronic information. The options are:

Option 1. Centralize Federal activities relating to safeguarding unclassified information in Government electronic systems under the National Security Agency.

Option 2. Continue the current practice of de facto NSA leadership for communications and computer security, with support from the National Bureau of Standards.

Option 3. Separate the responsibilities of NSA and NBS for safeguard development along the lines of defense and nondefense requirements.

The bill currently being considered by Congress (HR 145) is a variation of option 3 and is an attempt to resolve, by legislative means, policymaking for information security. One of its principal results is that it would clarif y the roles of NBS and NSA, and tend to separate civilian and defense interests. Among its main shortcomings is the absence of a capability to support unclassified research in safeguard technology. This capability, perhaps more than any other single factor, would strengthen the ability of the private sector to satisfy its own needs for information security and reduce dependence on the Government.

In option 3, additional choices can be made.

A. Provide Federal support to the private sector to specify, develop, and certify safeguards for business and civilian agencies. NBS would be the focal point for all safeguard standards for unclassified information; NSA would remain the focal point for classified information.

B. Allow free market forces to develop safeguards for nondefense needs, with NBS acting as the focal point for Government needs for safeguards for unclassified information. NSA would satisfy the requirements of Department of Defense agencies and their contractors, and provide technical advice for other users.

Each of the three broad options has shortcomings. Essentially, the choice depends on whether policymakers prefer to tolerate greater tensions, a blurred division between defense-intelligence and civilian matters, and more constrained private sector technical capabilities, or to take larger risks that intelligence capabilities will be damaged by proliferation abroad of U.S. safeguard technology.

OTA's evaluation indicates that centralizing authority in NSA for developing safeguards for unclassified information in Government systems (option 1) or maintaining the current, blurred relationship between NBS and NSA (option 2) would be the least effective in minimizing tensions and in separating defense and intelligence missions from civilian matters. On the other hand, U.S. foreign signals intelligence gathering operations may be poorly served if NSA is not party to all safeguard development (option 3).

Independent of institutional arrangements in the United States, however, there are also risks to our intelligence that stem from sources outside the control of U.S. policy, such as the policies of foreign governments, actions taken by international business interests, and the effects of foreign innovation.

There are inherent tensions between U.S. intelligence interests and evolving nondefense needs for information security technology. In addition, there are enduring conflicts involved in balancing national security and broader national interests. Potential conflicts also exist between the tendency to restrict access to unclassified, but sensitive information, and concern for the free flow of information and constitutional rights. Perhaps the optimum result that legislation should be expected to achieve is to provide a clear policy basis against which to measure future imbalances.

In addition, any option that raises the cost of safeguards, impairs user operating efficiency, or results in incompatible standards for defense and non-defense users, will discourage the development and use of commercial products.

There are no options for Federal policy that clearly and simultaneously foster all national objectives without costs to others. The alternatives for implementing policy differ mainly in the source of national leadership for the development and nondefense use of safeguard technology, the level of Federal encouragement or control of private sector innovation, and in flexibility to adjust to changing needs of commerce and society.

For policies to meet the evolving needs of the Nation, they will have to be flexible and balance various national interests.

Three main observations result from OTA's analysis:

1. Excessive accommodation of either commercial or defense and intelligence concerns could prove damaging to overall U.S. interests.
2. Policies that are inflexible, based primarily on defense and intelligence interests or on Government control of technological advances in the private sector, are likely to create substantial tensions with the widening range of other national and international interests affected by them.
3. A process for weighing competing national interests is needed. Centering policymaking in the Department of Defense alone and, in particular, NSA would make that difficult.