Chapter 7

Federal Policy Issues and Options

CONTENTS

Table

Chapter 7

Federal Policy Issues and Options

INTRODUCTION

Policy formulation in the area of information security is important today and will become more so in the coming decade and beyond. Its importance stems from the broad impact of electronic information on society and the potentially major applications of safeguard technology for commerce and government.

As discussed earlier in this report, applications of information safeguard technology are already being adopted to improve the efficiency, integrity, and control of business and Government automated transactions, and to improve their confidentiality as well. Much larger and more pervasive applications for commerce and society are foreseen, further stimulated by continued advances in this technology.

The Influence of Federal Policies

Federal policies can have a strong influence on the development and use of information safeguards. Policies may encourage private investment in safeguard technologies or, on the other hand, can discourage such activities. Chapters 5 and 6 provide a number of examples of policies and programs that have a combination of these effects. For example, the Government can stimulate the use of safeguards by setting technical standards, requiring specific message authentication and verification procedures for certain applications, and issuing performance guidelines and specifications.

On the other hand, secret Government designs for safeguards may result in high-qualit y, federally endorsed commercial safeguards, but discourage independent innovation in the private sector. Secret designs also foster private sector dependence on the Federal Government for equipment validation and certification, and the provision of replacement designs.

In the defense and intelligence communities, however, Government controls are seen as vital to U.S. signals intelligence interests. Technical and other controls on access to unclassified, but sensitive information in automated systems are being considered as a means for regulating the export of valuable information to foreign interests.

Federal policies require adjustments over time as the external environment changes. During an earlier era when protecting Government-classified communications from foreign exploitation was virtually the only objective, policies shaped exclusively by this need went unchallenged and tensions with other national objectives were nonexistent or minimal. Now, however, the objectives of Federal policy are increasingly expanding to include nondefense interests, such as the prevention of embezzlement of electronic funds transfers, the disruption of public services (e.g., air traffic control and Social Security transfer payments), and the theft of proprietary information from U. S.-owned firms by foreign competitors. At the same time, the expansion of earlier policies centered on national security and Government controls is creating tensions with other national interests. Thus, new objectives are becoming important and a different balance for Federal policy may be more appropriate.

Factors Influencing Information Safeguard Developments

How and when society fully realizes the potential benefits of information safeguard technology will be determined by a number of factors. One is the aggregate need of users. We can anticipate two effects from those needs: 1) that private sector users will increasingly set the pace in new applications of safeguard technology; and 2) that market forces will respond to user demand for new products, absent Government-imposed constraints.

A second factor concerns the net effect of Federal policies on stimulating private sector developments. Federal policies to date have helped some developments in computer and communications security technology and hindered others. (See chs. 4 and 5.)

A third influence concerns private sector innovation itself. The occurrence and rate of innovations is unpredictable. Important advances, such as public-key cryptography, have occurred without Federal encouragement. Yet, Federal policies can affect the climate for creativity by stimulating research or, alternatively, creating a chilling effect.

In this view, Federal policies have a significant, but not the sole influence on private sector developments. Nevertheless, they are particularly important because today's technology is still immature and market demand limited and, in some cases, fragile. Therefore, the policies of nations that are at the forefront of technological development and innovative applications, such as the United States, will have a major impact on the pace and direction of private sector advances in information security.

The National Security Influence in Policy Formulation

An analysis of information security issues in a report based entirely on unclassified data is hindered by a number of factors, one of which is the strong influence of classified information in shaping policy development. Neither Presidential Directive/National Security Council 24 (PD/NSC-24) nor National Security Decision Directive 145 (NSDD-145), for example, were debated openly. In fact, they were classified while being developed, although eventually unclassified versions were issued. Thus, the process of policy development, at least within the executive branch, has been a relatively closed one.

Secrecy is also an important factor in policies concerning the development of cryptography. Unlike other safeguard technologies useful in computer security, cryptography is the mainstay for providing confidentiality and integrity of information that is unprotected by physical or hardware/software security measures (as when such information is in transit on a network). Cryptography allows the United States to safeguard its classified defense and diplomatic communications. The absence of high-quality encryption in foreign communications makes possible some U.S. signals intelligence operations. Because of these defense and intelligence community interests and the general lack of nondefense interests in earlier times, public policy concerning cryptography has tended to be shaped and controlled by the Department of Defense (DoD).

Until recently, policy directions based exclusively on national security concerns adequately served the Nation's needs, with little visible impact on the rest of society. That situation is changing, spurred in large part by new opportunities and challenges created by technological change, continued pressure to improve business and government operations, and the emerging internationalization of applications of this underpinning technology. This changing environment also is likely to bring further challenges to policy makers as the needs of society continue to change both in the United States and abroad.

Interrelated Federal Policies and Changing Concerns

National security interests clearly have an important and continuing place in Federal information security policies. The prospect of worldwide use of high-quality information security safeguards threatens U.S. signals intelligence operations, as does the dissemination abroad of critical technical data on information security. As technology continues to advance and as safeguards for computers and communications systems come into wider use worldwide, the effectiveness of U.S. signals intelligence may become more limited and its priority lowered among national objectives.

Another policy involves control of access by foreign governments to commercial databases in the United States that contain unclassified,

but sensitive information. On-line databases allow rapid access and sorting through a wealth of information. Defense and intelligence agencies seek to prevent foreign intelligence agencies or businesses from acquiring valuable technical data that can help other countries compete with the United States militarily or economically.

Government concerns about communications and computer security, signals intelligence, and controls on foreign access to unclassified information change with time. PD/NSC-24, for example, elevated attention about the vulnerability y to misuse of communications systems to Federal policy status. Now, there are a number of DoD programs, some of which are classified, to reduce those vulnerabilities. Similarly, computer security was just being identified as an area warranting Federal concern in the early 1970s. Today, substantial resources are being applied to bolster computer security. Now, concern is extending to encompass access to Government databases, such as the Defense Technical Information Center and the National Technical Information Service.

Still another change is foreseeable. For example, the proliferation of information security technology could further broaden the scope of national security concerns. Within a decade, good quality, inexpensive, easy-to-use computer and communications safeguards may be used worldwide for many applications. That could shift attention away from the central national security issues of today, possibly toward countering the use of secret transactions for conducting illegal or subversive business.

Almost at the same time that these changes in Federal concerns have been taking place, the trend in private sector users' needs for information security can now be seen as overlapping some of the Government's applications requiring message authentication, user verification, auditing of transactions, confirmation of authorizations, and confidentiality.

POLICY ANALYSIS

The preceding sections and chapters raise questions as to the appropriate overall objectives of Federal policies, the direction in which current policies may lead, and whether or not other alternatives might better serve the Nation's interests. Based on the needs of the different stakeholders, e.g., businesses, scientific organizations, and civil, defense, and intelligence agencies, it is clear that each would provide a considerably different perspective to an analysis of policy options.

Important Trends for Policy

Chapter 6 described some of the Government efforts during the past few decades to solve particular problems through controls on unclassified information. In recent years, Government efforts have included restrictions, for example, on the dissemination of unclassified technical reports from the National Aeronautics and Space Administration and potential restrictions on access to Government information of the National Technical Information Service and the Defense Technical Information Center, as well as access to information in commercial database services. Thus, there has been a tendency in Federal policy toward greater control of selected information and, recently, of access to information in certain types of systems. Some of these policies have not recognized the needs of the public.

Because computers, information systems, and communications networks are changing so rapidly, policies based only on current needs are likely to become outdated quickly. Policies are needed that are flexible and anticipate the changing needs of industry and society. The factors discussed below are among those that are changing. They will significantly influence future policy deliberations, either because of changes in the policy environment or because of the public's attitude about Federal policies

that affect business operations and the free flow of information. Each provides insights into future directions for policy.

- Although some important improvements are foreseeable in the confidentiality of public communications systems, these are likely to be uneven. Many segments of these systems will remain vulnerable to exploitation by those with appropriate resources.

  To the extent that DOD programs depend on encouraging businesses to pay independently for reducing the vulnerabilities of their communications against Soviet or other foreign government interception, failure is likely since business profits are not perceived to be affected. There are strong indications, however, that some nondefense users will have business reasons to protect the integrity of certain of their information in computer and communications systems and the confidentiality of selected communications. Both interests can be served with cryptographic-based safeguards.
- A broad range of techniques for safeguarding unclassified information in computer systems and networks are available or are being developed. Private sector capabilities to develop these safeguards to meet their own needs are significant and expanding.
- Academic researchers and businesses have begun to demonstrate a level of expertise in developing certain types of cryptographic-based safeguards (e.g., the Data Encryption Standard and two-key systems). Further developments in this field are unpredictable. However, based on recent experience, Federal support for private innovation through unclassified research could yield promising results. Any additional major advances may also result in still more valuable new applications.

  These trends highlight a serious dilemma for Government policymakers: How to maintain effective signals intelligence while simultaneously encouraging the development and use of more secure systems for communications and computer systems. For example, encouraging unfettered private sector innovation in cryptography increases the chance of major technological advances that benefit commerce and society. But perhaps another country will use the same technology to protect its own electronic information from U.S. intelligence operations. On the other hand, if the National Security Agency (NSA) provides nondefense users with safeguard technology, the foreign interception and access threat may be reduced earlier, but the ready availability of "adequate" solutions from NSA may act as a disincentive for the private sector to develop solutions better tailored to its unique requirements.
- Although the current trends are not yet altogether clear, there are indications that businesses have diverse and specialized needs for cryptographic-based systems and other safeguards for a variety of nondefense applications.

  Almost certainly, no Federal agency will be able to satisfy the diverse needs of many of these users with Government-designed systems, especially if significant constraints must be placed on users.

  Private sector capabilities for developing computer and communications safeguards can meet most of the demand of Government agencies and other users. For the procurement of other commercial products, the typical practice among Federal agencies would be to provide their specific performance requirements and to purchase competitively. The arguments favoring a central role for DOD/NSA in carrying out these responsibilities are becoming less convincing, although there is a clearer need for NSA technical assistance in selected areas, such as cryptanalysis and equipment evaluation.
- Flexible Federal policies with minimal restraints are likely to have abetter chance of success than others. The banking industry's experience with NSA's planned restrictions indicates that Govemment-pro-

vialed safeguards, with rigid restraints associated with their use, are not likely to satisfy the needs of business users. (See ch. 5.)
- There is international demand for improved safeguards and foreign capabilities for developing them. (See ch. 5.)[1]
- DoD efforts to restrain or monitor foreign access to commercial on-line databases have already raised public concerns. (See ch. 6.) Further, these services are becoming a significant industry in the United States and a source of U.S. exports.[2]

Government efforts to control access to commercial databases are likely to continue to be resisted by this rapidly growing, competitive industry.

Today, NSA appears to be attempting to retain as much control or influence as is practical in these matters. The controls are exercised mainly through authority provided under NSDD-145 and various NSA programs, including those that stimulate the availability of commercial safeguard products. Yet, the above trends suggest that Federal policies concerning the development and use of safeguard technology, and access to unclassified, but sensitive information in commercial databases, will have to be carefully aligned with changing and more intensive domestic and international business interests and with congressional and other institutions.

Some businesses are unaffected by DoD initiatives, such as those that improve the confidentiality of common carrier communications systems or that require Government-reimbursed voice protection equipment to be used by defense contractors when discussing unclassified, but sensitive information by telephone. Still other businesses are likely to support Government initiatives that enhance their operational needs, such as Federal endorsement of data encryption algorithms and certification of commercial safeguard equipment. But others are likely to oppose any Federal policies that detract from trade, innovation, open science, and civil liberties.

Finally, there are questions raised about which branch of Government should make policy on information security. Both the executive and the legislative branches have adopted policies that show few signs of coordination. The executive branch has been most active in recent years, notably with NSDD-145, and the defense and intelligence communities, specifically NSA, have been the principal implementers. Executive branch policies have been based primarily on national security considerations.

National Values and Objectives

Because there are important stakes at risk for the Nation in formulating policy for safeguarding information, Congress has to carefully consider what the Government's broad goals are that these policies seek to protector encourage. 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 civil agencies for safeguard technology,
- minimize risks to U.S. signals intelligence from private sector developments, and
- clarify the roles of Federal agencies concerning unclassified information and the development and use of technology to protect it.

At the same time, achievement of the following, more general goals may also be desirable:

Ž promote competition, innovation, and trade;
Ž separate, where practical, defense and in-

[1] Richard I. Polis, "European Needs and Attitudes Toward Information Security' (unpublished), Telecommunications Policy and Research Conference, Airlie, VA, Sept. 30, 1987.

[2] These companies had revenues of $3.65 billion in 1984. Christopher Burns and Patricia Martin, "The Economics of Information, 1985, OTA contractor report No. 433-9520.

The industry had 486 companies by 1986. The number of database producers worldwide increased from 221 in 1979 to 1,500 in 1986, while the number of databases increased from 400 to 3,200 during that same period. OTA staff interview with Kenneth Allen, Information Industry Association, February 198'7.

telligence agencies' responsibilities from those of the private sector and civilian agencies;
- retain a free flow of information and an open society, while encouraging privacy; and
- minimize or reduce the tensions between Federal policies and private sector activities.

Levers for Implementing Policy

A number of incentives and constraints can be used to implement policies regarding safeguard technologies. These include programs to certify vendors' equipment, transfer technology, standardize designs, procure devices, and encourage the development and use of improved safeguards. Controls on exports and patents are clear examples of constraints. The funding of research by the Government can be either a constraint (e.g., by keeping the results classified) or an incentive.

Depending on how some of these levers are actually used, they could simultaneously promote and restrain private sector activities. Current Government practices in transferring cryptographic technology to the private sector appear to accomplish both. They also illustrate how policy levers can be used. For example, providing a few manufacturers with high-quality, inexpensive, tamper-proof, Government-certified cryptographic devices whose design is secret may meet the immediate needs of private sector users and vendors for certified systems. Simultaneously, national security objectives are served by encouraging the use of improved safeguards. In addition, the Federal Government can control the export of these products, in part because the underlying technology is produced by a limited number of U.S. companies for NSA. At the same time, however, this approach discourages further private sector innovation since it is unlikely that many users will want or that manufacturers will produce competing products that lack NSA certification and have limited demand.

Also, some policies may encourage continued private sector dependence on the Federal Government while others are more likely to lead toward an independent technical competence in the private sector for meeting its own needs. These effects are treated in more detail in the subsequent section that evaluates alternative policy options.

The focus of decisionmaking, however, is on the respective roles of NBS and NSA, and implementing policy around these roles.

Alternative Policy Options

Several options exist for national policy. They can be distinguished mainly by the degree of centralization within the Federal Government, the level of involvement in or control of private sector activities exercised by the Government, the separation of defense and nondefense interests, the importance of national security, and the flexibility of the private sector in developing information technology safeguards to meet its needs. Table 14 illustrates the options in their main division of responsibilities between the National Bureau of Standards (NBS) and NSA.

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.

In Option 3, additional choices can be made.

A: Provide Federal support to specify, develop, and certify safeguards for businesses and civilian Government agencies. NBS would be the focal point for all safeguard standards for unclassified information. This option most closely resembles HR 145.

Table 14.—Policy Options

Responsibilities for developing standards	Option 1 Centralize under NSA	Option 2 Continue current practice	Option 3 Separate defense and nondefense	Option 3A Support private standards development	Option 3B Market forces for unclassified needs
All classified	NSA	NSA	NSA	NSA	NSA
Unclassified					
Communications:					
Defense	NSA	NSA	NSA	NBS	NBS
Nondefense	NSA	NSA	NBS[a]	NBS[a]	NBS[a]
Computer:					
Defense	NSA	NSA	NSA	NBS	NBS
Nondefense	NSA	NSA	NBS[b]	NBS[b]	NBS[b]
Key distinctions	Centralization, NSA leadership	NSA defacto leadership	Mixed technical leadership	Commonality with non government safeguards	Commonality with non government safeguards Private sector leadership

[a]Refers to NBS's communications security standards responsibilities affiliated with computer security
[b]Refers to NBS's standards responsibilities under the Brooks Act (Public Law 89-306)

SOURCE: Office of Technology Assessment 1987

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 specifies the requirements of DoD and defense contractors and provides technical advice for other users.

The discussion of these policy options assumes that NSA would retain responsibility for matters relating to classified information in computer and communications systems under all options and that complementary NBS and NSA activities would be coordinated as necessary.

Options 1 and 3 would clarify the present confusion concerning the roles of NSA and NBS. Option 1 would provide one focal point in the Federal Government for efforts to develop safeguard technology for unclassified information in Government systems. This option would make use of NSA's technical expertise in cryptology and would concentrate the focus of U.S. policy toward national security objectives. The role of NBS in safeguard development would either be terminated or reduced to those civilian agency requirements that support NSA's role.

Option 2 would continue the current conflicting authorities assigned to NBS and NSA. It would also continue the current practice of NSA having de facto leadership in developing communications and computer security standards for the Nation, including increasing dominance over the development of cryptography. NBS would retain its current modest role in developing occasional, consensual technical guidelines and standards for civilian agency use.

Option 3 would assign to NBS responsibility for developing safeguards for all Government agencies' needs other than those specifically assigned to NSA. NSA would provide technical assistance to NBS, as needed. Under this option, NSA would be responsible for only those safeguard standards and developments required exclusively by defense agencies.

Option 3A would look to a nongovernment group or organization to take a lead role in developing consensual guidelines and standards for safeguarding unclassified information in private sector and civilian agency systems. Both NBS and NSA would actively support these private sector activities. NBS would serve as the focal point for civilian and defense

agency standards for safeguarding unclassified information. As in Option 3, NSA would be responsible for providing advice to the nongovernment standards group.

Option 3B is similar to Option 3A, except that the Federal role would be diminished further. It would abandon Federal responsibilities for developing safeguards for unclassified information and, instead, would look to the market place to meet both private sector and civilian agency requirements. NBS would serve as the Government focal point for the needs of Government agencies for safeguards for unclassified information.

Evaluation of Options

The national values and objectives described earlier provide a useful starting point for comparing the policy options. It is apparent that:

> The ability of the private sector to meet its own needs is fostered as the Government increasingly allows the marketplace to satisfy agencies' needs. In computer security, where industry and the private sector have historically led, NSA's trusted computer security program has benefited from significant manufacturer input. In cryptography, the commercial communication security endorsement program has limited the scope of manufacturer innovation of encryption algorithms, reflecting the historical NSA domination of this technology. In the area of network protocols, the interface between computer security and cryptography, there has been significant "give and take" between NSA and the private sector parties directly involved in the development of standards.

On the other hand, U.S. signals intelligence capabilities would be better–protected if control of private sector developments in (cryptography-based) safeguards are centralized under NSA. In the extreme case of relatively unfettered free market forces, there is a risk that signals intelligence will suffer as foreign intelligence targets benefit from safeguard products or designs developed by U.S. industry. Other factors that will affect the transfer of technology abroad include the effectiveness of U.S. export control regulations and the availability of comparable technology from foreign sources.

The current situation, which has produced considerable controversy and confusion, is essentially Option 2. Almost any option would represent an improvement in clarifying the roles of NBS and NSA. This is true whether responsibilities are centralized in one agency or divided according to divisions such as classified and unclassified information, defense and nondefense, or almost any other scheme.

Diminishing NSA's role is likely to reduce tensions between Federal policies and private sector activities in safeguard development and use. Similarly, such tensions are likely to decline as defense and intelligence interests are separated from nondefense interests.

Each of these options have other advantages and disadvantages that distinguish them. None offers a completely favorable assessment based on the objectives against which they are being evaluated. For example:

Option 1:

Pros: The key advantage that distinguishes Option 1, in addition to clarifying the responsibility of the National Security Agency, is the ability to maximize NSA's control over private sector activity in safeguard development, particularly those based on cryptography. That will allow it to minimize the risks to U.S. signals intelligence from independent private sector developments. Option 1 would be preferred if signals intelligence were the only or even the predominant policy consideration.

Cons: The main disadvantages are the likely affects of blurring defense and intelligence and civilian interests, and raising tensions due to differences in needs. Option 1 would probably have a stultifying effect on private sector innovation. The latter problem is most likely to occur in cases where new developments of value to society are detrimental to intelligence operations. The absence of a Federal standard for public-key cryptography, in spite of its obvious need, is an example of the effect of such a conflict.

Option 2:

Pros: This option retains most of the advantages of Option 1 while retaining a civilian agency

to interact with private sector users, vendors, and standards organizations. In this role, NBS would maintain an awareness and perhaps advocacy of the needs of civilian users.

Cons: Perhaps the most prominent shortcoming is the lack of clarity between the roles of NBS and NSA concerning information security. In the current situation, NBS has statutory responsibility for the development of computer security standards and for serving as the Government's representative in technical standards organizations. At the same time, NSDD-145 has assigned similar responsibilities to NSA, which is charged with reviewing and approving all standards, techniques, systems, and equipment for telecommunications and automated information systems security, This option also suffers from the problems of Option 1.

Option 3:

Pros: The division of responsibilities clarifies the roles of NBS and NSA, and provides for separation between defense and nondefense needs. This option also affords an opportunity to consolidate the Government nondefense needs with comparable needs of the private sector and to reduce tensions between defense and intelligence interests and those of the private sector.

Cons: The main shortcoming of this option concerns a lessening of NSA control of private sector innovation and its potential for damage to U.S. signals intelligence capabilities. This option also risks diluting a market that is already fragile by encouraging the adoption of different standards for defense and nondefense applications.

Option 3A:

Pros: Option 3A also would promote competition and private sector competence to meet its own needs and reduce tensions through increased Government dependence on and alignment with industry standards.

Cons: The main shortcoming, once again, concerns the potential damage to U.S. signals intelligence capabilities.

Option 3B:

Pros: The advantages are similar to those of Option 3A, but Option 3B further frees market forces and makes the Government dependent on the private sector rather than the other way around.

Cons: As in Option 3A, the main shortcoming is in potential damage to U.S. signals intelligence operations.

There are other factors for Congress to consider in evaluating the options. These include the resources required to carry out agency responsibilities under the various options, the need to carry out extensive coordination with commercial users and others in the development of standards, the ability to *engender the* trust of users, vendors, scientists, and others, and the ability to carry out needed research to benefit users generally.

It should also be recognized that NSA's technical expertise will bean important part of any of the options, e.g., evaluating safeguard techniques and equipments, especially those employing cryptographic methods.

As a practical matter, the resources available to NBS and NSA have not been comparable. NBS's budget for computer-related security standards has been about $10 million or less during recent years, and a staff of about 10 professionals, while NSA's National Computer Security Center alone employs some 300 people. (NSA's budget is classified.) For options in which NBS or NSA have a significant role in standards development, their efforts need to be coordinated with the needs and activities of the private sector. Although this study has not attempted to estimate the resource requirements under any of the options, some options would require changes in the funding levels of either or both NBS and NSA. In addition, it can be anticipated that any significant increase in responsibilities for the development of information safeguard technology will suffer from start-up problems, such as maintaining a high level of staff expertise, as has been the experience at NSA's National Computer Security Center.

There are a number of assumptions implicit in some of the options. One is that public acceptance of NBS standards would be based on the open scrutiny and consensual decisions that usually accompany the workings of civilian agencies. This assumption may not apply to NSA in a comparable standards-setting role

75-921 0 - 87 - 6

given the secretive way the agency normally operates and its unilateral decision to replace DES with a secretly developed algorithm.

None of the options make allowance for conducting research. Yet, OTA's analysis indicates that society's evolving information needs depend on continuing innovations in safeguard technology. Based on observations of the rapid acceptance of DES and public key cryptography for business applications, it seems clear that there are ready applications for innovations but a limited supply of them. For now, NSA is the main source of innovation in the Federal Government. However, its signals intelligence mission is likely to prevent the dissemination abroad of U.S. innovations. Because of this constraint, innovations generated by NSA may not be made available to the public at all.

Generally, there has been little motivation for industry to sponsor long-term research from which it cannot benefit on a proprietary basis. However, the quality of proprietary cryptography tends to be suspect by some U.S. critics.[3] In this situation, the Government may decide to undertake research into selected safeguard technologies. Research into cryptographic technology is likely to raise concerns for national security if undertaken openly by NBS and concerns about public trust if undertaken secretly by NSA.

There is also the practical question of how effective restrictions imposed by the United States on its citizens might be' if foreign innovations, publications, and product manufacture and export are not subject to comparable restraints.

Policy Observations

There are no options for Federal policy that clearly and simultaneously foster all national goals without harming some. The alternatives differ mainly in which Government agency leads in the development of safeguard technology, the level of Federal encouragement or control of private sector innovation, and in flexibility to adjust to changing needs of businesses and society.

Three main observations result from OTA's analysis:

1. None of the policy options simultaneously satisfy all objectives.
2. Excessive accommodation of either business or defense and intelligence concerns could damage overall U.S. interests.
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.

[3]There are, however, indications that many Western European businesses find proprietary cryptography acceptable, according to consultant Cipher Deavours. OTA staff communications, May 1987.

[4]Richard I. Polis, "European Needs and Attitudes Toward Information Security" (unpublished), Telecommunications Policy and Research Conference, Air-lie, VA, Sept. 30, 1987.