NTIA-CR-81-10

IMPACTS OF FEDERAL P
OPTIONS FOR NONMIL
CRYPTOGRAPI

contractor reports

U.S. DEPARTMENT OF COMMERCE National Telecommunications and Information Administratio

NTIA-CR-81-10

IMPACTS OF FEDERAL POLICY OPTIONS FOR NONMILITARY CRYPTOGRAPHY

VICTOR C. WALLING, JR.
DONN B. PARKER
CHARLES C. WOOD

PREPARED FOR:

NATIONAL TELECOMMUNICATIONS
AND INFORMATION ADMINISTRATION
U.S. DEPARTMENT OF COMMERCE
WASHINGTON, D.C.

SRI PROJECT 1663

U.S. DEPARTMENT OF COMMERCE
Malcolm Baldrlge, Secretary

Bernard J. Wunder, Jr., Assistant Secretary
for Communications and Information

JUNE1981

EXECUTIVE SUMMARY

Several developments in electronic technology are dramatically increasing private-sector and civilian government interest in cryptography. The growing use of information and communication systems is creating nonmilitary requirements to help assure privacy, security, and protection of information property rights. The assumption that only the military and diplomatic corps have major legitimate needs for high-quality crytography is no longer valid. Civilian applications from electronic funds transfer to protection of trade secrets to assurance of confidentiality of records all require ever higher quality nonmilitary cryptography. However, meeting these needs may jeopardize some current practices of the national security system (narrowly defined as military and diplomatic security activities).

To reconcile these interests, it is desirable to adopt a new principle as the basis for national policy toward nonmilitary cryptography. This new principle is that when considering whether to restrict or encourage nonmilitary cryptographic products and research, the contributions they make to the nonmilitary sector and to national security (broadly defined to include social and economic health and strength) should be balanced with any potential threat they pose to national security, narrowly defined.

Recent congressional attention has focused on the conflicts between segments of the private sector and the defense establishment concerning the publication of research results, patenting of inventions, export of hardware and technical data, and control over government funding of unclassified research related to cryptography. These conflicts have raised questions as to how much and what kind of government control is

reasonable and necessary, whether controls might have an undesirable "chilling effect" on related areas of research, whether statutory authority exists or should exist to support various controls, and whether First or Fifth Amendment rights prohibit certain controls.

Aggravating this conflict is the advancing international trend to use cryptographic technology to promote nonmilitary electronic system security and facilitate electronic information management. Moreover, the conflict level will escalate unless some reconciliation of overall U.S. interests is achieved.

Recognizing the importance of this growing problem, in December 1979 the Chairman of the Special Subcommittee on Telecommunication Protection of the National Security Council requested that the Secretary of Defense and the Secretary of Commerce propose a suitable national policy on cryptography.

A. A Framework for Issue Formation

The conceptual framework to address this issue is the emerging role of "electronic system integrity" in the nonmilitary (as well as the military) sector. The term "system integrity" refers to both (1) security, asset protection, and reliability and (2) effective accounting control of negotiable assets and information property rights. Electronic system integrity is ever more important to the nation as it becomes an information economy. For example, computer and communication safeguards help make possible secure interbank transfer of money electronically, or allow credit card users to have access to their financial resources through automated tellers; electronic transaction controls make it possible to sell scrambled (encoded) broadcast programs directly to individuals.

B. The Effects of Current Policy

Because today's federal policy concerning cryptography is oriented almost exclusively to current narrowly defined national security concerns, there has been limited consideration of why federal support of independent private-sector competence in cryptography may be necessary and desirable within the coming decade.

Today's policy structure, based on an adversary relationship, assumes that national security interests and independent nonmilitary interest in cryptography are necessarily in significant conflict. However, the national security, more broadly defined, may be increasingly threatened by the growing vulnerability of civilian electronic communication and information systems.

Yet, despite policy restrictions, there continues to be progress in development of nonmilitary cryptography through corporate, academic, and civilian government research. NBS and IBM, with assistance from NSA, developed a national Data Encryption Standard algorithm (DES); and the government continues to support development of standards to assist in the implementation of the DES.

C. The Costs and Benefits of Cryptography

Cryptography, properly used in an overall security system, would significantly reduce civilian system vulnerability to loss or disruption and potentially increase the value of these systems as backup for diplomatic and military uses.

Civilian cryptography is creating dramatic new opportunities for innovation and invention of new electronically based products and services that rely on powerful, low-cost system integrity. Signature encryption, for example, opens many possibilities, including improved integrity in contracts management, new forms of electronic purchasing, and electronic polling and voting. This opens a wide potential for

creating entirely new forms of business, including new forms of legal transactions.

The cost of powerful cryptographic algorithms and automated key management strategies integrated directly into system hardware will become virtually negligible on a unit-of-hardware basis within 5 to 10 years.

D. Results If The Present National Course Is Left Unchanged

Contention between civilian and narrowly defined national security demands for cryptography will grow. (There will also be a growing issue within the national security community concerning the scope of the national security threat from increasingly insecure civilian electronic communication and information systems, both public and private.)

Losses, disruptions, and costs of forgone opportunities to create new information services, products, and efficiencies in civilian electronic systems will increase.

From the perspective of total public and private benefit (outside current national security definitions), there will probably be underinvestment in basic research into system security and electronic information property rights management. This will occur because many of the benefits are diffuse and not proportionate in private economic markets to the business risks that suppliers must take (e.g., privacy and confidentiality of personal and business records are two such areas of large but diffuse potential benefit). This underinvestment may be especially severe before the development of national technical standards for the integrity of public communication networks and before development of more specific standards for duty of care in the protection of privacy rights and data in electronic communication and information systems.

Some technological and service industry leadership will be lost to foreign competitors as the security of their civilian electronic systems begins to match or exceed that of U.S. systems.

Some disruption of the rate and direction of progress in other sciences and technologies will result as researchers are discouraged from exploring cryptography-related concepts and as industry is discouraged from developing independent capability to provide high quality system integrity.

E. The Federal Government and Electronic System Integrity

Because cryptography is an effective, efficient, and often necessary means of providing the system integrity needed in our emerging information society, SRI came to one central conclusion concerning management of national cryptography policy:

> The federal government has the obligation to balance the value of meeting the growing need for nonmilitary cryptography with Department of Defense (DoD) concerns and efforts to constrain cryptography. This obligation should extend to federal facilitation of private sector efforts toward electronic system integrity research and product development.

Some of this federal obligation is being discharged under current policy. The National Science Foundation (NSF) supports basic science, and cryptography has many roots in basic science. The National Security Agency (NSA) provides communication security for military and diplomatic services and is seeking authority to provide grants for private-sector research in cryptography. The National Bureau of Standards (NBS) develops technical standards for civilian government use and helps facilitate standards that may be necessary to foster trade.

But there is no well-thought-out national strategy for federal facilitation of commercial electronic system integrity. This strategy should be based on all significant national needs, military and

nonmilitary, pertaining to national security in both narrow and broad terms.

Within this strategy of facilitating the evolution of electronic system integrity, current cryptography policies should be realigned to promote both national security, broadly defined, and encourage private-sector competence in designing and applying secure systems. Realigned policies that do not require legislative change might include:

- Increased encouragement of open, unclassified system integrity research, including cryptography.
- Continuing government support for development of national technical standards for cryptographic equipment and for its proper adoption and use.
- Continued government facilitation of standards of care in the areas of privacy and asset management in electronic systems.
- Limitation of International Trade in Arms Regulations (ITAR) export restrictions on cryptographic equipment to those products representing genuine leading-edge technology, and only when these are significantly superior to available foreign commercial products.
- Limitation of International Trade in Arms Regulations (ITAR) controls on cryptographic technical data to specifications associated with products or equipment categorized as leading-edge technology, and only when these data would effectively transfer manufacturing know-how significantly superior to available foreign technology. Use of ITAR to constrain scientific talks and technical publications should be avoided.
- Application of the Invention Secrecy Act only to cases in which the government has demonstrated that the national security threat of disclosure exceeds the potential social, economic, and technical benefits. This process should include balanced representation from the national security and nonmilitary interests in cryptography. The act should be applied only through a procedure that provides prompt assistance to the inventor in revising the patent application to avoid the secrecy order, if possible.

F. Policy Sutmnary

In view of the rapidly expanding nonmilitary need for enhanced electronic system integrity, the U.S. government policy on cryptography should be characterized by:

- Explicit procedures to balance the nonmilitary social, economic, and technological cost and benefit impacts with the expected national security costs and benefits, both narrowly and broadly defined.
- Awareness of foreign scientific progress and product development in the field of cryptography.

Implementation of this type of policy would be facilitated by reconciliation of national -security interests with the reality of growing world wide civilian need and capacity to provide electronic system integrity. 'lllis reconciliation could take the form of a new or expanded federal mission concerning computer and telecommunication systems security designed within a conceptual framework of electronic system integrity. Such a mission should be designed to bridge the gap between civilian and military concerns by encouraging the national security community to stay informed of the state of ·the art of civilian technology while preserving and encouraging civilian efforts. With few exceptions our respondents felt that the civilian sector interest in cryptography should be clearly and distinctly recognized and represented in federal policy and regulations •

ACKNOWLEDGMENTS.

During this project, more than 60 experts from the United States and Europe were kind enough to share their views with us on one or more aspects of this topic (Appendix A). We thank them, particularly those 11 who attended our July 1980 workshop (Appendix B). We also thank the more than 15 SRI experts in various related disciplines whose comments and criticisms were most helpful (Appendix C).

Positions taken by these individuals were in general agreement on the actions needed to facilitate nonmilitary cryptography but disagreed sharply on the forms any controls should take and the extent to which the nonmilitary sector could or would take these actions voluntarily. In presenting a synthesis, this report deliberately avoids making reference to the comments of particular individuals. Some individuals expressed strong reservations to some of the specific positions held by the majority of our interviewees. In such cases we have presented both positions.

Finally, we thank Mr. Charles Wilk and Mr. Donald Kraft of NTIA, and Dr. Fredrick Weingarten of OTA for their assistance, thoughtful participation, and critique of our work in progress.

The SRI authors take sole responsibility for the statements made in this report. It is a synthesis of viewpoints, not a description of a position arrived at by consensus. It is the opinion of the SRI project team that on many dimeusions of this matter no consensus can be obtained, not only because many of the facts are national security secrets but because there are fundamentally different perspectives on the relative significance of the various threats and opportunities that

nonmilitary cryptography presents. In this respect the national policy on this topic must be fundamentally a value decision on the type of society we want to live in and on how we want to defend it.

CONTENTS

I INTRODUCTION

A. The Problem

The nation faces a significant policy transition forced upon it by the rapid revolutionary changes in communication and computer technology.

Nonmilitary cryptography systems and research are attracting important attention from academia and commercial enterprises. This increasing civilian attention to cryptography is a direct result of three forces. First is the very rapid change in electronic communication and information technologies made possible br integrated semiconductor technology. Specifically, development of commercial microprocessors in 1971 began a new era in which increasingly powerful computers could be built very inexpensively and made widely available. Second, perhaps because of powerful inexpensive computing, cryptography research and development by commercial and academic sources has advanced rapidly in recent years. Third, there is growing civilian government and private-sector interest in enhancing privacy, security, and control of information property rights for their computing and telecommunication systems.

The potential economic and social contribution of cryptography-based security and information property rights management in this new era of electronic systems is extremely large. Information system integrity directly affects productivity, balance of trade, personal privacy, reduction of crime, and overall national welfare and security. Yet, at the same time international .pr·oliferation of cryptography, from foreign as well as U.S. sources, may jeopardize some of our present national security signals intelligence activities.

The growth of interest in nonmilitary cryptography has sparked a major policy debate: to what extent the Federal government should tolerate or encourage open nonmilitary research in cryptography. The new information technologies have created requirements for communication and file protection, both in civilian government agencies and in the private sector. This need in turn has led to unprecedented academic and commercial progress in cryptography related topics. For example, dozens of cryptography related scientific papers have been published in the past 5 years (mostly by Americans but also by foreign nationals), and more than two dozen firms are now offering cryptographic equipment. Various private businesses and civilian agencies are beginning to see a need for cryptographic protection for their computerized information systems and telecommunications. Some government agencies are also finding themselves with new responsibilities for protecting the personal privacy of Americans; other agencies are charged with responsibility for developing appropriate technical and procedural standards to promote privacy and asset security in electronic systems. The need has led to the adoption of the first national "Data Encryption Standard" (DES) by the National Bureau of Standards for government use and possibly general commercial use. These activities represent a substantial growth in nonmilitary concern for cryptographic research and development. This increased public interest conflicts with traditional practice. In the past private-sector advances were tightly controlled because almost all applications of cryptography were limited to military and diplomatic missions. This new conflict caused a comprehensive new policy for cryptography to be sought by the Chairman of the Special Subcommittee on Telecommunication Protection of the National Security Council in 1979.

Because the microcomputer revolution is so new its implications for society are not yet clear, and therefore, great care should be taken to base national policy about cryptography on forward looking values and national goals. Policy decisions should not be based on values and goals established to suit a previous era of technology. Retarding civilian cryptography may slow the rate of innovation and development of security and information property rights management strategies in

electronic communication and information systems. It may discourage research in their supporting sciences. This effect in turn could cause serious harm to the ability of the United States to remain globally competitive in civilian telephony, computer, and information-service industries. Moreover, it may also create major disadvantages should the United States decide in the future to place greater defense emphasis on securing civilian as well as military communication and information systems. In cryptography as in many other technologies no single theme represents the overall national interests.

The basic message of this report is that development of an appropriate national policy on cryptography should be made only in the context of a balanced consideration of the following three elements:

(1) The contribution that nonmilitary cryptographic research and product development can make to the American economy and the quality of life for American citizens (e.g., jobs, privacy protection, international competitiveness, control of crime, preservation of free speech, and freedom of research).

(2) The contribution that nonmilitary cryptography can make to national security, in the broadest sense of the term (especially as we move into the era of the electronically based global information society).

(3) The threat that nonmilitary cryptography poses to national signals intelligence and communication security as they are currently being conducted.

Because the project was designed to be unclassified, this report addresses the first of these three topics and focuses on the impacts of nonmilitary cryptography research on American society.

B. Objectives

Under contract to the National Telecommunications and Information Administration (NTIA), SRI International undertook this study with the following objectives:

(1) To evaluate the nonmilitary and nondiplomatic impact of altering the rate and direction of cryptographic research and new product development.

(2) To evaluate the impacts of federal policy on the rate and direction of cryptographic research and development.

This study had a very limited scope. No classified data or potential impact areas concerning the U.S. intelligence community were to be examined. However, a large number of our interviewees commented that national security might benefit significantly from independent and prolific development and use of very powerful cryptography in the nonmilitary sector. "Independent" does not mean without NSA knowledge. Without exception, our interviewees agreed that it is desirable for NSA to keep and be kept fully current on all new cryptographic technology and its deployment. Respondents were divided on the value and effect of direct involvement in or control of civilian cryptographic efforts by NSA.

II THE CURRENT POLICY

Currently federal government policy which affects nonmilitary cryptography research springs from two sources; traditional national security concerns, and concerns for government facilitation of commerce and basic science. National security concerns have led to the ITAR, (the International Traffic In Arms Regulations, 22 CFR Parts 121-128) (Sturges, 1980), the Arms Export Control Act of 1976 (22 USC 2778) and the Invention Secrecy Act (35 USC 181-188), which have been and continue to be used to limit the distribution of American cryptographic technology to other nations and to limit the U.S. patent rights of American inventors (but not of foreign inventors). Federal concerns for commerce and basic science, particularly to meet public and federal civilian needs, have led to federal grants and standards development activities in the area cf cryptography or in fields of basic science that have proven to yield significant cryptographic insight (for example Public Key Code technology was discovered and developed by academic researchers supported in part by federal research dollars). Moreover there has recently been effort by NSA to develop both a prepublication review process for cryptogru•hy related research, and to devise and support its own unclassified cryptography grants program. Table 1 summarizes this current policy situation. (Appendix D presents a review of current policy status. Appendix E lists the primary legal underpinnings of current policy.)

Within this policy context, however, conflicts have begun to arise between new and traditional interests. This conflict is well documented in the House Government Information Subcomittee Hearings (1980). Some national security community representatives have declared that proliferation of nonsecret cryptographic research capability constitutes

TABLE 1 ·
CURRENT POLICY

PoucY AREA	Pou CY Pos IT ION	IMPACTS
EXPORT RESTRICTIONS	ITAR AND ARMS EXPORT CONTROL Ac T CONTROL EXPORT OF EQUIPMENT AND TECHNICAL DATA	• REQUIRE CRYPTOGR LICENSE ENCOURAG COMPETIT
INVENTION SECRECY	PATENT OFFICE ISSUES SE- CFECY ORDERS AT REQUEST OF DEFENSE AGENCIES (DoD, NSA, DoJ)	SECRECY ORDERS (MORE TH
PREPUBLICATION REVIEW	FORMALLY REVIEW ON PROJECTS OUTSIDE DoD FUNDING, IS NOW TRYING A VOLUNTARY PROCEDURE	OPEN INT OF NON-D RESEARCH
FEDERAL FUNDING LEVEL.	NSF FUNDS WORTHY OF BASIC RESEARCH INCLUDING SOME CRYPTOGRAPHY NSA SEEKS STATUTORY AUTHORITY TO PROVIDE GRANTS FOR PRIVATE SECTOR RESEARCH	NSF SUPP SCIENCE DRAWS U ACADE CRYPTOGR ONA SERI
TECHNICAL STANDARDS	BRooKs AcT LED To DESt	ONE NATI STANDARD SUSPICION

a significant threat to their mission, and that greater restraints and control by DOD are therefore necessary (Inman, 1979). Many researchers in the academic community argue that even the present restraints are too severe, not only because they have a chilling effect on the amount and type of cryptographic research but because reduced research in turn deprives Americans individually and collectively of products and services that could increase their privacy, personal security, and even national security (Helman, 1978).

In response partially to the concern for the system security requirements brought on by the new electronic technology, Congress took one key direct action in the form of the Brooks Act (1965, PL 89-306) to support development of standards for government use of computers. This act combined with the requirements of the Privacy Act of 1974, helped lead NBS to adopt the DES.

This action did not end the conflict, it expanded the controversy. Suspicions were immediately voiced that if NSA found the DES acceptable for widespread use, then NSA must be able to break it either through a trap door or by testing (Diffie 1978). This suspicion was reinforced by the fact that some of the specifications of the DES were not made available to the public for evaluation and criticism.

Overall, this incident points up that the demand for cryptography in the nonmilitary sector cannot be met simply by supplying one good multipurpose algorithm. A part of this sector demands the opportunity to independently evaluate the quality of any code proposed for use and to do so in an atmosphere that is open and above suspicion, particularly for products designed to serve in the international market.

A basic philosophical conflict that goes even deeper than that between current military and nonmilitary interests in cryptography concerns adequate secure-system design. One side says that the details of a security strategy should be kept secret to increase its effectiveness. The other says that, at least for commercial systems,

unless the security strategy is designed overtly, its weaknesses will not come under the most effective criticism; hence, the system will be weaker and more vulnerable to attack than it could be.

In this context of current controversy, policies in six areas are coming under discussion. These policies and their most immediate impacts are cited in table 1, "Policy Situation Today" and discussed in more detail in Appendix D.

The current policy situation concerning cryptography reflects the traditional concerns of the national security community, although it is debated whether these policies are adequate to satisfy this community's interpretation of its needs. Conspicuously absent as a principle for establishing national policy, is any direct recognition that there is a legitimate and growing need for nonmilitary cryptography capability and that this places an obligation on the federal government to balance the value of nonmilitary cryptography with any national security value from constraining it. This means, for example, that some agency should be specifically assigned the task of representing and facilitating public interest that is served by improving electronic system integrity including nonmilitary cryptography. Some agency should be assigned the mission to identify and facilitate private sectors research and development for those national nonmilitary cryptography needs not otherwise adequately reflected in private market forces.

III THE RATE AND DIRECTION OF THE EMERGING CIVILIAN NEED

The role of cryptography in society has been changed by three basic forces: the rapidly growing need for electronic system integrity, the potential rapid decline in cost of system-integrated cryptography, and the growing importance of many of the various sciences on which cryptography advancements depend.

A. The Need for Systems Integrity

The general purposes of encryption (and other safeguards) are to help protect data from misuse, abuse, errors, and omissions and to provide transaction control. Table 2 displays the types of interactions for which cryptography is relevant. Transaction control is used to assure orderliness, integrity, auditability, and accountability in electronic markets involving data as intellectual products and negotiable assets (such as electronic money). In the electronic exchange of assets in both form and speed, encryption is of increasing importance as a means of control as well as safeguard. Then the exchange and accounting of decryption keys to convert the encrypted information back to plaintext form completes the transaction. For example, the distribution of electronically based educational or entertainment programs (television, radio, computer interaction, and the like) can take place through mass distribution in encrypted form. Accounting for use of the programs can be accomplished by an exchange of money for keys through a brief telephone exchange. This makes it possible for audiences to buy what they would like directly rather than through support of advertisers' products.

One of the most promising cryptographic concepts to facilitate

TABLE 2

EMERGING CRYPTOGRAPHY ROLE IN E

USES	TYPES OF ACTS		EXAMPLE APP
	CAUSE	EFFECT	
PRIVACY PRESERVATION		MODIFICATION	RECORDS - M
		ERRORS	- CRE
		OMISSION	
		DESTRUCTION	MONEY - EFTS
			- Po IN TRA
Loss PREVENTION	ACCIDENTAL	DISCLOSURE	MESSAGES- T
			- ELEC
	INTENTIONAL	REMOVAL	- PRO
		UsE	Copy- RIGHT - SU
		DENIAL OF USE	BRO
			- PAY
TRANSACTION CONTROL			
ELECTRONIC INFORMATION PROPERTY RIGHTS MANAGEMENT			

THREATS CRYPTOGRAPHY HELPS PREVENT I

OF TRADE SECRE FRAUD IMPERSONATION DE CE

transaction control is that of the digital signature. Development of public key cryptographic strategies has greatly enhanced practical application of this concept. By encrypting the message with a secret key as the signature of the author, digital signatures may make possible virtually tamperproof electronic documents. This technique has many applications; for example, it makes it possible to create legally binding contracts and signatures authorized at a distance and communicated electronically.

Protection from errors and omissions is usually treated as a serendipitous benefit of encryption. There are more effective means of direct protection from accidental loss. However, this inherent benefit increases the attractiveness of encryption. Error and omission detection and correction based on early work of Shannon and Hamming in information theory, use concepts employed in encryption. This is another example of the overlap of research between cryptography and other important research subjects.

Abuse and misuse have been identified as potential threats for which encryption can be a particularly valuable safeguard. Here it is important to distinguish between protection of data from criminals and protection of their own data by criminals. Therefore, abuse and misuse form two types: (1) direct loss to legitimate owners and custodians of data through modification, destruction, disclosure (including taking), and unauthorized use or denial of use, and (2) use of encryption for criminal and other antisocial purposes.

Some examples of direct loss to legitimate owners and custodians that is preventable with encryption are:

(1) Transferring funds from several accounts into a favored account in a bank checking account system.

(2) Inserting a fictitious employee record into a payroll file.

(3) Modifying the names and addresses of stockholders in a dividend payment system.

These activities can be done using a master program that can change the contents of data files independently of the production program that is authorized for processing the files. The master files could be encrypted and decrypted under control of the production program which generates its own encryption key. The files would be available in plaintext, one record at a time, only during authorized production processing. If this action were taken, the remaining serious vulnerability appears to be unauthorized modification during the production program operation or unauthorized modification of production data input.

(4) Inserting data into a communication circuit to allow repeated withdrawals of cash from an automated teller machine using and magnetic stripe card and personal identification number.

This activity would be especially complex and would require great skill and knowledge even in the absence of encryption. However, encryption could make it totally impractical relative to the potential gain. Currently in some EFT systems data sent over the communication circuits is encrypted during transmission. This adds complexity to the job of the attacker. He must break the encryption processor obtain the encryption key. Otherwise, the perpetrator is forced to gain access to the control data before encryption in the computer or after decryption in the automated teller machine.

(5) Destruction of invoice data that would have shown removal of products from a warehouse.

If the invoice data were block-encrypted in computer storage media such as cards, tape, or disk, then any kind of meaningful destruction of selected data would also destroy easily detected amounts of other receipt data; the decryption process would then reveal that the original data had been modified. Therefore, for the crime to occur, the receipts would have to be destroyed before or during input to the computer or during output from the computer.

(6) Retrieval and display of trade secrets from a computer ata remote terminal.

Trade secrets could be encrypted in computer storage. Authorized terminal users would have secret identifiers to prevent theft by others.

This protection would also help preclude those authorized to use the computer frc;,m gaining unauthorized possession of the plain.text material without leaving a clear audit trail. Therefore, the perpetrator must either capture the trade secrets in the computer as plaintext, or obtain the encrypted information and attempt to decrypt it.

(7) Taking a mailinglist of mostfavored customers.

(8) Obtaining personal medical recordsfrom a hospital records systemfor use by insurance salesmen.

These activities could be precluded by routine encryption of the data whenever they are not being used for authorized purposes. Breaking the encryption process or key and obtaining the key from the authorized custodian remain as the likely vulnerabilities.

The above cases show that encryption, considered in the broad context of computer and communication security, replaces one set of vulnerabilities with another. In some cases the use of encryption does not reduce the greatest vulnerability (such as bribing a computer operator) and is therefore ineffective in protecting the whole system against an observant and intelligent enemy who can find and take advantage of opportunities that are easier and safer than defeating an encryption system.

Therefore, encryption will be effective only when it strengthens the weakest, most vulnerable links in an information system and when it is part of a comprehensive safeguarding effort.

Some examples of the use of encryption for criminal purposes are:

- Safe communication and storage of betting information in a bookmaking operation.
- Use of a time-sharing computer for safe communication of informat;l.on concerning .criminal activities such as drug traffic or prostitution.
- Secretly encrypting the financial master files and backup files of a company in its own computer .and holding the key for ransom.

The above cases show that making encryption generally available for

legitimate purposes makes it available for criminal and other antisocial purposes as well. One result is that extensive use of encryption by criminals may reduce the value of court-ordered wiretapping by law enforcement agencies, currently a valuable tool in fighting crime.

B. Uses of Encryption

For purposes of prevention of abuse and misuse and transaction control, encryption can be used for concealment, source authentication, and data authentication. Each of these is discussed below.

Concealment -- Disclosure of data to unauthorized parties can be prevented. The contents of misrouted messages therefore will not be divulged to mistaken receivers of these messages. In addition, the volume of data, its source, receiver, timing and frequency of transmission can all be concealed.

Source Authentication -- Decryption into an intelligible plaintext indicates that the message probably comes from the supposed source. To the extent that it can be proved that the source is the authentic and only possessor of the key, that party is authenticated. Therefore, encryption can be a significant element of message source authentication.

Data Authentication -- If data in ciphertext form are modified in any way, decryption will reveal the modification, magnified by the decryption process.

Federal Requirements for Privacy and Legal Standards of Due Care

At the same time that these various vulnerabilities have emerged to create a need for new protections, there has been a rise in federal legislation to require increased protection and due care concerning citizens' privacy rights and rights to public records. Hence, legislation and regulation may become a major force to promote private-sector and civilian agency adoption of cryptography equipment.

(Typical laws that may be interpreted to have this effect include the Right to Firtancial Privacy Act of 1978, and the Family Educational Rights and Privacy Act of 1974.)

Because of growing private sector uses for cryptography, combined with federal requirements for electronic security, we conclude that in the absence of federal and international constraints on civilian cryptography, over the next several decades DoD will cease to dominate the market for cryptographic products. DoD may continue to dominate the cutting edge of the market in this country, but the private-sector will soon acquire and use a significant number of cryptographic devices.

C. The Declining Cost of Cryptography

Cryptography has two major subsets, cryptography and cryptanalysis. Cryptography is the use of a coding scheme, and cryptanalysis is the process of breaking the code. The cost of each of these is being powerfully affected by the semiconductor revolution. The hardware costs of implementing powerful cryptographic systems such as the DES is falling rapidly because semiconductor complexity is rising while the unit costs are falling. On the other hand, exhaustive search is a geometric function of the complexity of the cryptographic algorithm, hence the increasing complexity of cryptographic systems has a geometrically increasing impact on the cost and even feasibility of cryptanalysis. Our interview subjects all agreed that even the DES, if properly implemented to multiple-encrypt, would become unbreakable by any technique or set of hardware available in the unclassified sector today.

Over the next decade, an impressive degree of potential cost decline is highly probable for cryptographic systems implemented by direct integration into the electronic systems they are to serve. To build an encryption system such as one that uses the DES requires about 5,000 active devices (Diffie, 1978). In 1975, 5,000 devices were about the maximum that could be put on one chip. In 1980 there are more than

60,000 active devices on individual chips available commercially. According to SRI semiconductor industry experts, by 1985 the device count will reach 600,000, and by 1990 the count will exceed 2,000,000.

Today the DES is typically sold in an add-on device at a retail price of $1,500 to $3,000 installed. Integrated into a system as part of the original equipment, cryptographic algorithms such as the DES would become much less costly. The potential cost per unit of the next generation of algorithm after the DES, however may be virtually zero. If this generation algorithm can also be implemented using about 5,000 active devices, it will occupy as little as 0.25% of the surface area of the most advanced chips in 1990. This means that for those chips which probably cost less than $200 the cost of integrating cryptography will be less than $.50 per unit in large volumes (assuming the cost of integrating cryptography into the total chip logic is proportional and does not make it significantly more expensive.) Moreover, because the cryptographic algorithm will be physically in the same chip as the rest of the computer, data for such a device might enter and leave in encrypted form and be in plaintext form only within the chip itself.

While a rapid decline in costs of semiconductors can reduce the cost of a cryptographic algorithm implemented in hardware to virtually zero, it can also change key management costs. Key management is the task of maintaining the security of the encrypting and decrypting key and securing transmission of new keys between the encoder and decoder. Semiconductor technology, coupled with major advances in mathematics and computer science, has led to development of two key cryptographic systems that allow the encoder to publicly broadcast his encryption key without revealing his decryption key. Called "public key code" (PKC), this technology allows the process of key management to be fully automated; the economic and psychological costs of key management may therefore also be reduced.

Certainly, within a decade powerful integrated cryptograhic systems using automatic key management could be produced in mass quantities for

a marginal cost per unit of no more than a few-dollars.

The application of such devices in the telephone system, cable or fiber-optic systems, and even subscription broadcasting systems could create hundreds of new information service industries--for example, a records management industry that maintains personal records such as medical histories safely anri securely, while relieving physicians of the cost and complexity of office file maintenance. The records would always be encrypted before they left the doctor's office so that even the records managers would not have access to the plaintext.

D. Tbe Dependence of Cryptography on Other Sciences

PKC offers one example of the connection between cryptography and basic sciences. In this case the discovery and exploration of trap-door mathematical functions provided an ideal starting point to develop a two-key asymetrical code.

Because cryptography is a field that applies many concepts to a particular set of practical problems, it draws on a wide variety of other sciences. Key branches of science, in addition to mathematics, that are used by cryptographers include computer sciences, statistics, and human factors. The individuals in these fields, along with the colleagues they call on for review, can recognize when a new concept has cryptographic implications. It is also possible to identify the common concerns shared by cryptographers and scientists in these other fields. These common grounds range from finding shortcuts in complex computations to finding human factors that affect the interface between human users and computers. In particular, cryptographers and mathematicians share a common interest in developing general proofs as to the type and degree of complexity of a given mathematical problem.

In the future we can expect even greater dependence of cryptography on other sciences that are highly critical to many sectors of our society. Two areas of dependence are likely. First is pattern

recognition technology that would coincidentally allow people to use some personal characteristic (such as the face) as their unique cryptographic key. Second is computer-aided design which will allow designers to further reduce the cost of building system integrity directly into electronic systems.

IV PREREQUISITES FOR ANALYSIS OF FEDERAL CRYPTOGRAPHY POLICIES

There are three major factors that interact to constitute a policy impact: the nature of the impact, the value of the impact as seen from someperspective and the framework thatputs the impactin the context of the other events and values in the society. The approachused in this report for each of these is described below.

A. The Nature of Impacts from Alternative Federal Cryptography Policies

The range ofimpacts of policies aimed at maintainingor altering the rate and direction of cryptographic research or product development is quite broad. Cryptography and the policy leversnecessary to control it have increasingly broad and deep connections toa large number of services and products that affect civilian life (Business Week, 1981).

Table 3 lists 12 impact categories that are affected by changesin the rate and direction of nonmilitary cryptography research and development or by changes in federal cryptography policy.Under each category are selected specific impact dimensions (national security impact categories have.been deliberately excluded). The purpose of this table is to show how broadly varied were the impact areas mentioned by our interviewees.

Impacts of a policy fall iµto three basic types. The first is direct intended impacts, for example, the direct' success or failure of a policy designed to prevent criminal use of cryptography. For example, the U.K. requires that the key be registered with the government before any encryption is done over the nationaltelephone network. The second

TABLE 3
IMPACT AREAS OF CRYPTOGRAPHY POLICIES
(EXCLUDING NATIONAL SECURITY)

1	2	3	4	5	6
DOMESTIC PRIVACY	DOMESTIC SECURITY	DOMESTIC SOCIAL ECONOMIC WELFARE	DIRECTION OF ACADEMIC R&D ON CRYPTOGRAPHY	DOMESTIC CRYPTOGRAPHY INDUSTRY	GENERAL RESEARCH IN THE U.S.
I GOVERNMENT INTERFERENCE	I TRADE SECRETS	I PRODUCTIVITY	I NUMBER OF RESEARCHERS	I SALES	I ACADEMIC FREEDOM
I INSTITUTIONAL INTERFERENCE	I FRAUD PREVENTION	I QUALITY OF LIFE	I RESEARCH TOPICS	I EXPORTS/ IMPORTS	I DEVELOPMENT IN RELATED SCIENCES
I CRIMINAL INTERFERENCE	I TRANSACTION CONTROL	I SOCIAL NETWORK STRUCTURE	I TYPES OF RESEARCH INSTITUTIONS	I INNOVATION	I EXTENT AND BALANCE BETWEEN INVOLVEMENT OF DoD AND OTHER GOVERNMENT AGENCIES
	I DISRUPTIONS OF CONTROL SYSTEMS		I QUALITY AND AVAILABILITY OF TYPES OF CRYPTOGRAPHIC PROTECTIONS	I RATE OF NEW COMMERCIAL PRODUCT DEVELOPMENT	

7	8	9	10	11	12
LEVEL OF GENERAL PUBLIC DEBATE OVER CRYPTO	DOMESTIC GOVERNMENT FUNCTIONS	DOMESTIC IN-DIRECT IMPACTS	COMPETITION FROM NON-U.S. SUPPLIERS	INTERNATIONAL NONMILITARY STANDARDS	FOREIGN USERS
• FREQUENCY OF GENERAL PUBLICATIONS	I QUALITY OF SOCIAL SERVICES	I FIRST AND FIFTH AMENDMENT RIGHTS	I MARKET SIZE & SHARE	I SECURITY SYSTEMS (NETWORK TRANSMISSION MEDIA)	• HUMAN RIGHTS
• TONE OF GENERAL PUBLICATIONS	• POLICE ROLE I POLITICAL PARTICIPATION	I TRUST/ALIENATION	I RATE OF NEW PRODUCT DEVELOPMENT	I TRANSBORDER DATA FLOW (CONTENT)	I TOTALITARIAN POWERS I ATTITUDES TOWARD U.S. (INFORMATION IMPERIALIST)
			I ACCESS TO MARKET		

is direct unintended impacts, for example, the effect of a policy designed to prevent criminal use of crytography on the ease of legitimate use. Finally, there are indirect effects of the policy or second-order effects of its direct effects, for example, the impact on the frequency and type of invasion of the privacy of honest citizens because a policy to prevent criminal use of cryptography has also made it much more difficult or costly to use cryptography legitimately.

Hence, the path linking cryptography policies to impacts in these 12 impact areas is direct in some cases and indirect in others. Were the government to institute a process of mandatory prepublication review of all cryptography-related research papers, examples of the three types of impacts would be:

- Direct intended: Potentially some improved opportunity for DoD to stay fully informed and current on academic cryptography research progress.
- Direct unintended: Decline in graduate student interest in cryptography there by reducing the pool of qualifieq talent for recruiting by military and nonmilitary employers.
- Indirect: Slower improvement in nonmilitary electronic system security for want of qualified personnel.

B. Perspectives on the Value of Policy Impacts

Possibly never in our history has the U.S. citizenry been more polarized than today on many value issues. There are competing interest groups with contrasting perspectives on energy, the environment, gun control, welfare, integration, and many more issues. The same impact by a policy in one of these areas may be considered a benefit by one and a cost by another.

This conflict of values also pertains to national security and to the place of national security relative to other national goals and priorities. Hence, it is not enough to characterize only the nature of the impacts from alternative cryptography policies; it is also necessary to evaluate them from several value perspectives. Table 4 summarizes

Table 4

TWO VALUE PERSPECTIVES ON CRYPTOGRAPHY POLICY EFFECTS

Perspective A	Perspective B
Some national security requirements (narrowly defined) take priority over constitutional rights.	Preservation of full constitutional rights is the only justification for national security actions.
National security depends first and foremost on a strong military/diplomatic position.	National security depends first and foremoston a strong domestic economy and effective international exchange.
Nonmilitary electronic system security research and development should be controlled by DoD.	Nonmilitary electronic system security research and development should be independent of DoD and subject to international peer review.

two opposing value systems that our interviewees agree defines the spectrum. Certainly, there are more than two, but for the purpose of this analysis two are sufficient to present the argument for the role of values in selecting alternative cryptography policies.

C. An Analysis Framework

In light of the complexity of the impact categories and the reality of conflicting value perspectives on the impacts of nonmilitary cryptography, we developed a specific framework for analyzing alternative federal cryptography policies. See appendix I for an elaboration of the origin of this framework. The framework has two major components. First, it recognizes that cryptography as a concept and a technology cannot be separated from other safeguards for electronic communication and information system security. Policies aimed at cryptography will have immediate and direct effects on the entire domain of communication and information security. Second, it assumes that the policymaking process can generate a synthesis of values that incorporates and meets the major concerns of the different perspectives. We do not predict what this perspective would be but expect some of its characteristics to be:

- Reconciliation of the current national security concerns with concern over growing nonmilitary vulnerability and newly emerging forms of national vulnerability.
- Recognition of the growing importance of very high electronic system integrity for international competitiveness in information service and systems industries.

V POLICY IMPACTS

A. Objectives for Cryptography Policy

The objective of present federal cryptography policy is not to alter the rate or direction of U.S. cryptography development in and of itself, and it is not adequate to say that the objective of policy should be to increase or decrease the rate or determine the direction of nonmilitary cryptographic technology innovation. Choices of policy objectives in this area are more subtle. Options we found among our interviewees included emphasis on enhancement of:

- National security.
- Nonmilitary security (especially in communication and information systems).
- Individual quality of life in such categories as personal privacy and assurance of confidentiality.
- New techniques to manage information in the emerging "information economy."
- U.S. international competitiveness in service and information industries as well as in the computer and telecommunications hardware industries.
- Academic freedom and open communication in basic research.

The following discussion is divided into two major topics to respond to the two project objectives. The first discusses the impacts of altering the rate or direction of cryptography research and development. The second discusses the impacts of alternative federal policies to regulate cryptography research and development. The second also is divided into two parts: a discussion of the impact of current policies and a discussion of selected alternative policies. (Appendix H contains a list of likely impacts which were suggested in the course of our interviews.)

1. Impacts of Altering the Rate or Direction of Cryptographic Research

Later sections will discuss the impacts that specific policies might be expected to have. Here we present and evaluate the impacts that all policies successful in altering the rate or direction of cryptography R&D might be expected to have in common.

With the exception of the national security objective, impacts on each of the policy objectives are discussed below. We acknowledge that officials of NSA have gone on record saying that some types of uncontrolled cryptographic research and product development may have negative impacts on national security. On the other hand, many of our interviewees who volunteered comments on the national security issue suggested that there may be a rapidly increasing national security benefit to strong independent private-sector capability to safeguard the "new wealth" of the post industrial era. Significant national dangers were cited ranging from inadequate security against sabotage in the areas of electronic funds transfer, to unsecured national and international news services, and major public utilities such as power and transportation.

Concerning the other objectives it was generally agreed that to the extent that federal policy retarded the development of nonmilitary cryptography it would also retard U.S. progress toward these goals.

2. Impacts on Nonmilitary Security

Our interviewees suggested that at this point in time cryptography may offer little additional security in many theoretically useful applications. This is the case because there are typically easier ways today to abuse systems against which cryptography would offer little protection (such as bribing an insider rather t. han tapping a communication line.) However to the extent that security becomes tighter in various systems those links that can be protected by encryption may become the weak links. Moreover the terrorist and

criminal elements of our society have not yet had much time to develop their computer skills and learn how to attack information systems. As all of society becomes more "computer literate" we can expect that these groups will also become computer literate. Therefore more imagination and skill will be invested to attack and commit crimes against our information and computer systems.

It is not possible in advance to specifically measure the size of this risk or how much it may be increased or decreased by increasing or decreasing the availability of nonmilitary cryptography. (An approach to risk analysis is presented in appendix F.) However many examples of the potential danger can be given. It is conceivable, for example, that a small terrorist organization could coordinate (a) an attack on key international oil installations with (b) deliberate manipulation of unsecured international news services and possibly even with (c) some manipulation of international financial transactions to set off a major financial panic. In fact any one of these events might set off such a panic. It was not within the resources of this project to determine how severe such a panic could become. Many of our interviewees thought one or more of these forms of attack are entirely possible and that the vulnerabilities grow daily. Several individuals suggested that it is not only terrorists who might attempt to demoralize our economy through such an attack but also certain foreign powers or extremist groups.

3. Impacts on Individual Quality of Life

The principal impacts of changes in the type and availability of cryptography on the quality of life, according to our interviewees, were in the domain of privacy and confidentiality on one hand and in the area of potential new products, services, and employment possibilities on the other. Again, there was no agreement on the economic, social, or national security value of enhanced or decreased personal privacy, or on the value of the ability of government or private institutions to assure confidentiality of records or communication. Some examples were suggested of the costs of the present system's weaknesses ranging from threat of blackmail to inflated professional insurance costs to protect

against breaches of confidentiality. One interviewee proposed that cryptography concepts available today might easily allow professionals to turn over the task of maintaining confidentiality of client records to a sort of "Brinks" electronic security service integrated with a full line of electronic data processing services. Finally, one interviewee suggested that international diffusion of an inexpensive, powerful technology that guaranteed personal privacy and confidentiality in message exchanges clearly had a potential to improve the human rights struggle of many people.

It was generally agreed that many useful potential applications could be developed if nonmilitary cryptography were permitted and possibly even encouraged to develop in the world marketplace. No agreement was reached on the size of the benefit from these applications in the United States or in other nations.

4. Impacts on U.S. International Competitiveness.

Our respondees generally agreed that international sales of many information services, such as banking and some computer and telecommunications hardware, depend on the quality of the underlying system integrity. They also agreed that as security increases as an issue in system integrity, the cost and ease of cryptography use will be a characteristic to which the international market is sensitive. We found some sensitivity in our foreign interviews to the lack of independence of American cryptography technology from government--and specifically NSA--influence. Some interviewees believe that only security systems developed under open procedures without direct NSA involvement would sell effectively internationally; others said such involvement might make little or no difference.

5. Impacts on New Information Management Techniques

The impact of the rate and direction of nonmilitary cryptography research and development on new information management techniques is highly speculative because the value of innovations in this area is very difficult to anticipate. Two examples demonstrate the potential. First, in the area of pay or subscription broadcasting, encryption may make it possible to significantly enhance the variety and even the quality of education, information, and entertainment available in the home. The value of an orderly market that allows direct electronic purchases of specific information products from the home or office may have the same potential order of magnitude effect on society as did the invention of the printing press. Already, relatively crude forms of encryption are being used to permit pay television broadcasters to control access to their signals. On the other hand, piracy and other forms of property rights abuse are becoming serious threats to the entertainment business. Today many millions (possibly billions) of dollars in sales, much of it from overseas, are lost in this field. Cryptography may offer some solutions to help cut these losses.

A second example of how cryptography may offer a major invention to help expand productivity in the information economy lies in digital signatures. This is the application of cryptography to develop forgery-proof electronic documents and signatures. Such a technique might make it both possible and desirable to recognize electronically transmitted signatures as legally binding. This in turn could have major implications for improving efficiency in contract administration or increasing the range of flexibility in electronic or catalog sales. It could even be a contributing technology to permit more decentralization of work and increase the kinds of work that could be performed in the home.

Until the imagination of the commercial sector has had time to assess what cryptography can be used to do, it is not possible to estimate specifically how important nonmilitary cryptography may be as

source of or element in new information management products or services, however the importance is potentially very large.

B. Summary of the Impacts of Altering Cryptography R and D

Overall it is our judgment, based on our interviews and other research, that retarding the rate of nonmilitary cryptography development or limiting its independence would impose important restrictions on the areas of nonmilitary security, personal privacy and assurance of confidentiality, U.S. international coompetitiveness, and innovation in new information techniques. We also suspect that there may be important national security costs in retarding nonmiliary cryptography. To some extent, accelerating the rate of development of independent, nonmilitary cryptography would have the opposite effects.

Beyond saying that they are potentially quite large, it was not possible to estimate accurately the overall importance of these effects, for three reasons. First, there is little or no agreement on the precise size of each impact--for example, how much sabotage of international EFT might be prevented by cryptography or how great might be the damage if it were not prevented. Second, there is no agreement on the value of many of the impacts, even if their exact size could be specified. For example, there is no agreement on the value of privacy. Finally, the only useful standard for comparing importance of impacts is the simultaneous gains or losses in all the areas of impact, including national security; particularly because only in that context can adjustments be identified that would give maximum benefit and minimize costs across all contrasting perspectives.

Within these limitations we concluded that the federal cryptography policies to be preferred have the following characteristics:

(1) They permit the national security community to stay most currently informed of progress in nonmilitary cryptography.

(2) They permit and encourage independent, nonmilitary competence in cryptographic research and product development.

(3) They provide the type and degree of government support necessary to encourage a more rapid rate of technological change in system integrity development than would occur with private-sector support alone.

(4) They permit continued recognition that leading-edge cryptography technology (like sophisticated microprocessors) has a military strategic value and should be exported only under appropriate license constraints.

(5) They discourage controls on the export of technical data to the extent that controls would impede private sector research and development, innovation and domestic trade.

We again point out that these criteria were chosen without access to any classified information. There may be specific national security threats that we did not encounter in our interviews that would alter these priorities. It is within this limited context that we assessed specific policy alternatives to regulate cryptography.

VI IMPACTSOF ALTERNATIVE POLICY OPTIONS

A. Choices for the Future

One clear result of present trends is that we are being drawn to a basic choice concerning cryptography, in which we have three options. As a nation we can:

(1) Muddlethrough with no specific policy changes. This will satisfy neither the current national security concerns nor the civilian needs.

(2) Consolidate the federal support for electronic system integrity development, including cryptography, under one agency and assign that mission to DoD because of its necessary interest in military and diplomatic cryptography.

(3) Recognize that there is a new and growing civilian demand for system integrity, including cryptography, and create a civilian mission, distinct from that assigned to DoD for facilitation of development of civilian system integrity.

B. Probable Results of the Present Policy Course

The future of nonmilitary cryptography in the international context is being shaped by these forces:

(1) The growing use and dependence on electronic communication and information systems.

(2) The near technological parity and extreme competition in electronic products and services amoung Western Europe, Japari, and the United States.

(3) The rapidly declining cost and increased functional ease of use of cryptography in electronic systems.

(4) Several interviewees felt strongly that there is an increasing interdependence between the integrity of civilian communication and information systems and national security that may lead many nations to make such

greater use of powerful civilian cryptography. An evaluation of this topic is outside the scope of this project.

In addition to these international forces, the trends in cryptography in the United States are also being shaped by:

(1) A general atmosphere of government discouragement of private-sector interest or effort to develop independent competence in electronic system integrity, including appropriate use of cryptography.

(2) Sporadic and uncoordinated federal regulations concerning the amount and type of security and due care that must be exercised in fields of electronic communication and data processing ranging from securities exchange to maintenance of personal records.

For more detail on the status of present national cryptography policy see Appendix D.

Hence the present policy course will likely have these results:

(1) Contention between civilian and current national security demands for cryptography will grow. (There may also be a growing issue within DoD concerning the size of the national security threat from increasingly nonsecure civilian electronic communication and information systems.)

(2) Losses, disruptions and costs of foregone opportunities to create new information services, products, and efficiencies in civilian electronic systems will increase.

(3) From the perspective of overall social benefit (outside current national security definitions) there will be underinvestment in basic research into systems security and electronic information property rights management as measured against total social return from such research. This will be especially true prior to the development of national standards for the integrity of networks such as the Fedwire or for legal standards of due care in the protection of privacy rights and data in electronic communication and information systems.

(4) Loss of some technological and service industry leadership to foreign competitors if the security of their civilian electronic systems begin to match or exceed that of the U.S.

(5) Some disruption of the rate and direction other sciences and technologies as researchers are discouraged from exploring cryptography related concepts and as industry is not encouraged to develop its own independent capability to provide system integrity.

C. The Impact of One Centralized Federal Cryptography Mission

Extension of the current status of DoD as the centralized location of federal involvement in electronic system integrity development may have advantages from the current narrowly defined national security perspective. However, most of our interviewees did not think such a change would benefit the nonmilitary sector nearly as much as would recognition of distinct military and nonmilitary interests, for two reasons. First, centralization in DoD would tend to lead to more frequent classification of new ideas and hence would hold back new technology. Secondly, it would also tend to discourage the private-sector from developing the capability to diagnose and eliminate its own security vulnerabilities; at the same time, it would leave the suspicion that DoD-approved products must be of limited value. This approach would lead to less use of cryptography in the nonmilitary sector than would otherwise result, or to the use of cryptography in forms that are not optimized to commercial and civilian applications.

D. Alternative Policy Options and Impacts

There are five primary focal points for federal actions to alter the rate and the direction of cry&#65533;tography:

- Research
- Product development
- Domestic distribution and use
- Foreign distribution and use
- Publicity concerning cryptography research or products.

With these focal points in mind, a wide variety of types of policy options that could theoretically be applied were uncovered in the course of this project. Appendix G contains this list. From this

Table 5

LEVERS FOR FEDERAL CRYPTOGRAPHY POLICY

Target Area	Levers
Research	(1) Direct federal funding of research o The amount of funding. o The channels of funding. o The type of research organization funded, o The security classification associated with funding. o Prepublication review requirements. (2) Risks and incentives for private sector research o Patent and copyright restrictions. o Availability of highly skilled labor (scholarships and research money). o Size and type of ultimate market, o Cost of research,
Product Development	(1) Cost of new product development o Licensing and testing requirements, (2) Firm's ability to protect and recover its investment o Invention secrecy (especially administered with high uncertainty). o Limitations on the applicability or use of the product,
Domestic Distribution and Use	(1) Domestic standards o Algorithms (DES), o Protocols. o Key manag[illegible]ment. (2) Federal market for systems o Required characteristics of systems to be purchased by federal agencies.

	(3) Private market requirements o Characteristics that must be provided for assurance of civil rights, rights to property, etc. o Characteristics that must be provided to meet "standards of due care" requirements.
Foreign Distribution and Use	(1) Export controls (ITAR, Export administration controls) o Hardware constraints. o Technical data constraints - Blueprints, design, and algorithms. - Academic papers. - Scientific conferences. - Technical expertise. - Foreign nationals in U.S. research.
	(2) International standards o Quality for international and foreign national businesses and services. o Applications for cryptography systems.
Domestic Publicity	(1) Secrecy requirements.
	(2) Profile of DoD's public commentary.
	(3) Communication between DoD and the civilian cryptography community.

list a list of specific policy levers was synthesized for each of the five focal points for federal action (Table 5).

Based on conversations with our interviewees and several synthesis sessions at SRI, including a workshop on July 11, 1980, we made a basic assessment of the primary impacts of options for possible policy levers (see Appendix H). From this assessment the six basic policy clusters discussed in the remainder of this section emerged in response to the five major concerns.

1. An Alternative Policy Concerning Federal Cryptography Research Support

Because demand for cryptography is so new and the nonmilitary technology is not yet well developed, it appears desirable to continue federal support for such cryptography research for several reasons:

- A major demand for cryptography is being and will be created by government regulation. Nonmilitary cryptography research could help provide the knowledge to select better and less costly regulations regarding security in civilian electronic systems. Conversely, it may produce less costly ways of meeting nonmilitary regulatory goals.
- Major benefits of nonmilitary cryptography are likely to be diffuse or hard for product developers to capture through the price mechanisms of the marketplace. (This situation is common in new high-technology products.) To the extent that many social benefits of improved system integrity are not well reflected in market prices, federal support of R and D is necessary to produce a higher rate of technological innovation.

Therefore, we believe that the new federal policy on cryptography should provide INCREASED ENCOURAGEMENT FOR UNCLASSIFIED SYSTEM INTEGRITY RESEARCH, INCLUDING CRYPTOGRAPHY.

2, An Alternative Policy Concerning Private-Sector Competence in Cryptography

Because of the rapidly growing variety in the vulnerabilities of nonmilitary electronic communication and information systems, it is desirable to encourage the development of the private-sector competence to identify these vulnerabilities and take any prudent actions necessary to reduce them, This approach is appropriate for several reasons:

- It eliminates the need for the government to provide all the leadership and resource support for a private-sector activity that promises to advance technology.
- It permits the private-sector to operate openly with international peer review, and thereby compete more directly in world markets that depend on international confidence in electronic system integrity.
- It enables the national security community to maintain an arms-length relationship with nonmilitary security and to avoid becoming more the center of controversy over meeting this nonmilitary need,
- It would allow the nonmilitary market to develop along lines that best meet nonmilitary needs without unnecessary biases from government prerequisites,

Therefore, we believe that the new federal policy on cryptography should provide ENCOURAGEMENT OF INDEPENDENT PRIVATE-SECTOR COMPETENCE IN CRYPTOGRAPHY.

3. An Alternative Policy Concerning Development of National Standards for the Use of Cryptography

Because cryptography is becoming an important characteristic of electronic systems within domestic and international markets, and because these systems have broad social implications and uses, it is desirable for the federal government to continue a major participation in setting national and international cryptographic standards, Several specific government responsibilities increase the appropriateness of government involvement in standard setting:

- The Federal government is a major maintainer of records on individuals, The fact that these records should often be kept confidential makes the federal government a

potentially large buyer of cryptographic products and services. When the is a major buyer of a new product government procurement specifications sometimes become de facto standards for those products.

- The federal government sets standards in a number of fields relying on electronic communication and information systems, for example, electronic funds transfer and air traffic control. Hence, it is appropriate for the government to participate in setting standards to better coordinate regulations in these areas with alternative standards.

Therefore, we believe that the new federal policy on cryptography should provide CONTINUING GOVERNMENT SUPPORT FOR DEVELOPMENT OF NATIONAL STANDARDS FOR CRYPTOGRAPHIC EQUIPMENT, ALGORITHMS, AND PROTOCOLS FOR THEIR PROPER ADOPTION AND USE.

4. An Alternative Policy Concerning Federal Restrictions on Export Of Cryptographic Products

Because international and transnational nonmilitary applications of cryptography are likely to continue their rapid growth, the international market for cryptographic hardware is likely to grow. Also, the integrity of international electronic systems is likely to become increasingly important to international trade in information, communication, and financial services. It is therefore desirable to encourage U.S. suppliers to compete vigorously in the international electronic integrity market, for several reasons:

- Such competition will allow U.S. organizations to have a greater role in establishing international standards for electronic systems.
- Such competition will help eliminate a divergence in integrity maintenance strategies between U.S. nonmilitary organizations and their foreign competitors.
- Such competition will avoid leaving a market gap that might give a major advantage to foreign trade competitors in such areas as: - Computers (office automation and robotic controls) - Telecommunications - Communication and information services.
- Such competition will help avoid a situation in which the United States becomes a major (dependent) importer of foreign nonmilitary electronic system security technology.

Therefore, we believe that the new federal policy on cryptography should LIMIT ITAR EXPORT RESTRICTIONS ON CRYPTOGRAPHIC EQUIPMENT TO THOSE PRODUCTS THAT REPRESENT GENUINE LEADING-EDGE TECHNOLOGY, AND ONLY WHEN THESE ARE SIGNIFICANTLY SUPERIOR TO FOREIGN PRODUCTS.

5. An Alternative Policy Concerning Federal Restrictions on Export of Cryptographic Technical Data

Both for nonmilitary reasons and for stronger legal support of U.S. ITAR constraints on technical data, export restrictions should be narrowed to apply to product specifications or technical information that effectively communicate manufacturing know-how. Such constraints may be practical and enforceable because product specifications can be more clearly defined by legal precedent. Other forms of technological exchange, such as the exchange of academic papers, should not be constrained for several reasons:

- There is no clear, objective standard for determining when a piece of work on a topic is closely enough related to cryptography to warrant constraint.
- Constraints may hamper the free flow of ideas within the United States and hence slow domestic nonmilitary research progress.
- Constraints may be declared unconstitutional except where convincingly shown to represent a grave threat to national security (Harmon, undated).

Therefore, we believe that the new federal policy on cryptography should LIMIT ITAR CONTROLS ON CRYPTOGRAPHIC TECHNICAL DATA TO SPECIFICATIONS ASSOCIATED WITH PRODUCTS OR EQUIPMENT CATEGORIZED AS LEADING-EDGE TECHNOLOGY, AND ONLY WHEN THESE WOULD EFFECTIVELY TRANSFER MANUFACTURING KNOW-HOW SUPERIOR TO AVAILABLE FOREIGN TECHNOLOGY.

6. An Alternative Policy Concerning Invention Secrecy Constraints on Cryptographic Products

Invention secrecy orders for cryptographic technologies should continue in the short run if neccessary for national security, but only for those inventions that directly gravely threaten existing military or diplomatic communication security. The appeals process for inventors should be improved, not only to better provide due process for the inventor but also to assist the inventor in modifying his patent application so that it need not be classified. Such actions are desirable because they will:

- Reduce the uncertainty and risk of private-sector investment in new electronic system integrity research (and thereby reduce the public cost and increase at least the nonmilitary public benefit of such private research).
- Reduce the incentives for U.S. multinational organizations to move their system integrity research operations overseas.
- Reduce the differential incentive in the U.S. patent system to protect foreign invention property rights while potentially limiting the property rights of U.S. inventors of similiar products. (A foreign patent will be granted even though a secrecy order would have been issued for an identical U.S. patent application.)

Therefore, we believe that the new federal policy on cryptography should be to SELDOM IF EVER APPLY THE INVENTIONS SECRECY ACT TO CRYPTOGRAPHY, AND LIMIT APPLICATION TO CASES IN WHICH THE GOVERNMENT HAS DEMONSTRATED THAT CLEARLY THE NATIONAL SECURITY THREAT OF DISCLOSURE EXCEEDS THE POTENTIAL SOCIAL, ECONOMIC, AND TECHNICAL BENEFITS.

In summary, we believe that in contrast with current policy the new federal policy on cryptography should be tempered by:

- EXPLICIT PROCEDURES TO BALANCE THE PROPOSED NATIONAL SECURITY BENEFITS OF RESTRAINTS AGAINST SOCIAL, ECONOMIC, AND TECHNOLOGICAL COSTS.
- AWARENESS OF FOREIGN SCIENTIFIC AND PRODUCT DEVELOPMENT OF CRYPTOGRAPHY FOR THE NONMILITARY SECTOR.

E. Some Open Questions

Several questions important for establishing cryptography policy were left open in this inquiry, because of either limitations of scope or lack of reliable unclassified expert information sources. These questions include:

(1) What is the national security value of increased nonmilitary use of cryptography to eliminate vulnerabilities in civilian systems?

(2) How secure must a system be to be "adequately secure"? This question seems to come down to the dangers and costs associated with making the transition from an older, obsolete system to a newer one. If the costs and security threats of such transitions are very high, they should be minimized by using the best current technology and practice in each new installation or application (Diffie, 1981).

(3) What is the quality of foreign nonmilitary cryptography in terms of civilian market requirements? Because the cryptography markets are so new, their requirements are not yet well defined, nor are there international or even national commercial standards to measure performance. Conversely, there is no independent neutral authority (analogous to Underwriters' Laboratories) to provide an assessment of cryptographic products.

(4) In the absence of this authority, is there a need for the government to provide assistance or is it as some interviewees asserted that even current government assistance is retarding private sector development of needed capabilities?

(5) How rapidly will foreign suppliers fill the gap if the United States constrains its own cryptography development? The answer to this question depends on two factors: the current level of foreign nonmilitary cryptography development capability and the size of the incentive foreign suppliers perceive to fill the gap. In the opinion of our interviewees, the level of foreign capability to develop new cryptography technology is significantly behind that of the United States, but is closing fast, particularly because of the foreign students studying computer science and mathematics in this country. We gained little insight into how foreign companies view the incentives of the cryptography market, except that in Europe in particular, civilian cryptography is a well established small market, that has begun growing. Moreover, both the French and the Japanese have major national commitments to develop the

technology necessary to be leaders in telecommunication and information processing industries including the development of any necessary electronic system security and information management technology. A study conducted by NTIA (CRC, 1981) found 3 dozen vendors of cryptographic terminals worldwide; ten are foreign and four of these are headquartered in non-NATO countries (i.e., their sales would not be subject to multilateral member export restrictions). The largest of these, Crypto AG, uses a proprietary algorithm (all foreign suppliers use proprietary algorithms) which claims to be superior to the DEC. Crypto AG exports to over ninety countries.

(6) How much independence from NSA (in terms of technical competence and managerial confidence) is necessary for U.S. suppliers to be credible and meet the needs of foreign, domestic, and transnational markets? The answer to this question would require an in-depth analysis of the product marketing and purchasing strategies of both U.S. and foreign firms regarding electronic system security products.

(7) How quickly will the communication and information system links that can be protected by cryptography become the weakest links to major systems? This question is important because the transition point from one set of weakest links to another may mark the point of a sudden increase in demand for cryptographic protection. Our interviewees had no definitive answers. Some suggested that it depends on the timing of such breakthroughs as automated voice recognition.

VII CONCLUSIONS

SRI reached three basic conclusions:

First, broad and highly valuable applications for cryptography in the private-sector, though very recent in origin, are likely to grow rapidly over the next several decades. Hence it is desirable to reconcile national security interests in signals intelligence and communication security with the reality of growing, world wide civilian need and capacity to provide electronic system integrity. This reconciliation could take the form of a new or expanded federal mission concerning computer and telecommunication system security within a conceptual framework of electronic system integrity. The mission should be designed to bridge the gap between civilian and military concerns by encouraging the national security community to stay informed of the state of the art of civilian technology while preserving and encouraging civilian efforts. Experts consulted in this study agreed that the national security community should be provided with the resources to stay ahead of and build on civilian progress. With few exceptions, our respondents also felt that to one degree or another the civilian sector interest in cryptography should be clearly and distinctly recognized and represented in federal policy and regulations.

Second, the Federal mission and policy framework for cryptography should be designed to foster private-sector competence in providing what the marketplace determines is the necessary level of electronic systems security and property rights control. However, it may be necessary in the short run for the Federal government to augment market forces by defining legal requirements in such areas as required standards of care for assuring confidentiality in both government and private record-

keeping. it may also be necessary to set national and international standards concerning the minimum security effectiveness that systems must have to be used with various nonmilitary government files and personal records.

Third, given this framework cryptography policies should be:

- Increased support for open unclassified systems integrity research including cryptography
- Encouragement of private-sector independent competence in cryptography
- Continuing government support for development of national standards for cryptographic equipment and for its proper application and use
- Limitation of !TAR export restrictions on cryptographic equipment to those products that represent genuine leading-edge t[illegible]hnology, and only when these are superior to available foreign products. (This does not address political criteria for deciding on control of exports to selected foreign countries.)
- Limitation of !TAR controls on cryptographic(technical data to specifications associated with products or equipment categorized as leading-edge tecl1nology, and only when these are superior to available foreign technology. The scope of !TAR should be clarified and narrowly interpreted. Use of !TAR to constrain scientific talks and technical publications should be avoided because of their detrimental side effects and because it may violate First or Fifth Amendment rights. A mission to facilitate nonmilitary development and application of cryptography should include reviewing both the short-term and long-term nonmilitary costs of proposed !TAR applications.
- The Invention Secrecy Act should seldom if ever be applied to cryptography and should be limited to cases in which the government has demonstrated through timely due process that the national security threat of disclosure exceeds the potential social, economic, and technical benefits. This process should contain balanced representation from the national security and the nonmilitary interests in cryptography. The act should be applied through a procedure. that provides prompt assistance to the inventor to revise the patent application in ways that will avoid the secrecy order.

In view of the rapidly expanding nonmilitary need for enhanced

electronic system integrity, any U.S. government restriction on cryptography should be tempered by:

- Explicit procedures to balance the proposed national security benefit against the social, economic, and technological costs of the restrictions.
- Awareness of foreign scientific and product development.

BIBLIOGRAPHY

Adleman, Leonard M., and Ronald L. Rivest, "The Use of Public Key Cryptography in Communication System Design," IEEE, November 1978, pp. 20-23.

Alexander, Tom, "The Postal Service Would Like To Be the Electronic Mailman, Too," Fortune, June 18, 1979, pp. 92-100.

"Americans Are Worried About Loss of Privacy," San Francisco Chronicle, May 3, 1979, pp. 30.

"Announcing the Data Encryption Standard," Superintendent of Documents, U.S. Government Printing Office, Washington D.C.

"Associated Computer Industries Offers NBS Encryption," Infoworld, July 7, 1980.

"Banking by Computer - It Moves a Step Closer," U.S. News & World Report, March 7, 1977, pp. 81-82.

Beardsley, Charles W., "Is Your Computer Insecure?" IEEE Spectrum, January 1972, pp. 67-78.

Bell, Daniel, "Communications Technology--For Better or for Worse," Harvard Business Review, May-June 1979, pp. 20-42.

Berg, John L., "Exploring Privacy and Data Security Costs - A Summary of a Workshop," NBS, Washington, D.C., August 1975.

Blumenthal, Marcia, "Maintain Lead in Research or Lose Role as Leader, Packard Tells U.S. Industry," Computerworld, May 26, 1980, page 21.

Brandin, David H., "Public Cryptography Study Group--Interim Report No. 2," private communication to NSF committee members, June 25, 1980.

Branstad, Dennis, "Validation Tests for DES Devices," January 29, 1976.

Brenner, Steven N., "Business and Politics--An Update," Harvard Business Review, November-December 1979, pp. 149-163.

Brenner, Steven N., and Earl A. Molander, "Is the Ethics of Business Changing?" Harvard Business Review, January-February 1977, pp. 57-71.

Browne, Malcolm W., "Scientist Urges New Laws To Curb Misuse of Computer Technology," The New York Times, November 17, 1977.

Bruno, James N., "Electronic Mail: It Gets There Fast," Administrative Management, September 1979, pp. 28-70.

Bruno, James N., "Privacy: An Issue for the Eighties," Administrative Management, August 1979, pp. 33-36.

"The Business Stake in Soviet Snooping," Business Week, December 12, 1977, pp. 57-58.

Campbell, Duncan, "Whose Eyes on Secret Data?" New Scientist, March 2, 1978, pp. 593-595.

Canning, Richard G., "Data Encryption: Is It For You?" EDP Analyzer, December 1978, Vol, 16, No. 12, pp. 1-13.

Carter, Jimmy, "Proposal To Protect The Privacy of Individuals," Office of The White House Press Secretary, April 2, 1979.

CRC Systems, Inc., "An Assessment of Technological Trends Affecting the Development of Cryptographic Markets--Working Paper #1," prepared for U.S. National Telecommunications and Information Administration, February 15, 1980.

CRC Systems, Inc,, "An Assessment of the Market for Cryptographic Equipment--Working Paper #2," prepared for the U.S. National Telecommunications and Information Administration, February 29, 1980.

"Credit Cards Get A Lot Smarter," Business Week, February 23, 1981, pp 107-111.

"Cryptically Yours," The Economist (UK), February 1978, p. 92.

"Cryptography Meeting Goes Smoothly," Science, November 1977, p, 198,

Darrow, Joel W, and James R. Belilore, "The Growth of Data Bank Sharing," Harvard Business Review, November-December 1978, pp. 180-190.

Davis, Ruth M., "The Data Encryption Standard in Perspective," IEEE, November 1978, pp. 5-9.

Department of Justice, "Testimony of H. Miles Foy, Senior Attorney--Advisor, Office of Legal Counsel, Before the Government Information and Individual Rights Subcommittee of the Committee on Government Operations, House of Representatives," February 28, 1980, Washington, D.C.

Diffie, Whitfield, "Cryptographic Technology: Fifteen Year Forecast," BNR Inc., prepared for CRC Systems under contract from the U.S. Department of Commerce, January 1981.

Diffie, Whitfield, "The Outlook for Computer Security," Mini-Micro Systems, October 1978, pp. 42-44.

Diffie, Whitfield, and Martin E. Hellman, "Multiuser Cryptographic Techniques," American Federation of Information Processing Societies, National Computer Conference Proceedings, 1976, pp. 109-112.

Diffie, W., and M. E. Hellman, "New Directions in Cryptography," IEEE Transactions on Information Theory, Vol. IT-22, No. 6, November 1976, pp. 644-654.

"Discovery Rocks World of Math, Computers," San Francisco Chronicle, November 15, 1979.

Eger, John, "Transborder Data Flow," Datamation, November 1978, pp. 50-54.

Federal Reserve Bank of Minneapolis. "Electronic Funds Transfer--An Introduction," Ninth District Quarterly, July 1976.

Freundel, Mark, "Overseas Cryptographic Industry and Crypto AG," memo to Chuck Wilk, National Telecommunications Information Administration, June 16, 1980 (private communication).

Gardner, Martin, "A New Kind of Cipher that Could Take Millions of Years to Break," Scientific American, pp. 120-124.

Girsho, Allen, "Communications Privacy," IEEE.

"Grasping for Privacy," The Washington Post, April 7, 1979.

Harmon, John M., "Constitutionality Under the First Amendment of ITAR Restrictions on Public Cryptography," Dept. of Justice Memorandum to Dr. Frank Press (Science Advisor to the President), undated (private communication).

Hellman, Martin, "Cryptography in the Electronics Age," The Stanford Engineer, Fall/Winter 1978, pp. 4-82.

Hellman, Martin E., "An Overview of Public Key Cryptography," IEEE, November 1978, pp. 24-32.

Hindin, Harvey J., "New Security Planned for Data," Electronics, August 16, 1979.

Hiltz, Starr Roxanne, and Murray Turoff, The Network Nation: Human Communication Via Computer, Addison-Wesley Publishing Company, Reading, MA., 1978.

Hoffman, Lance J., Modern Methods for Computer Security and Privacy, Prentice-Hall, Englewood Cliffs, NJ, 1977.

Hoffman, Lance J., Security and Privacy in Computer Systems, Melville Publishing Co., Los Angeles, CA, 1973.

Horan, Thomas F., "Electronic Funds Transfer Systems," Business Intelligence Program - SRI International, Research Report 573, April 1976.

House Government Information Subcommittee Hearings, February 28, March 20, and August 21, 1980.

Inman, B.R., "The NSA Perspective on Telecommunications Protection in the Nongovernmental Sector," Signal, March 1979.

Kahn, David, "Cryptography Goes Public," Foreign Affairs, Fall 1979. pp, 141-159.

Kolata, Gina Bari, "Cryptography: A Secret Meeting at IDA?" Science, April 14, 1978, p. 184.

Kolata, Gina Bari, "Cryptography: On the Brink of a Revolution?" Science, August 19, 1977, pp. 747-748.

Kolata, Gina Bari, "New Codes Coming Into Use--Their Unique Properties Make Them Ideal for Tamper-proof Security Systems," Science, May 16, 1980, pp. 694-695.

Kolata, Gina Bari, "Solve One and You Could Solve Them All," New Scientist, April 3, 1980.

Lancaster, Hal, "Desktop Deception--Rise of Minicomputer, Ease of Running Them, Facilitates New Frauds," The Wall Street Journal, October 5, 1977, pp. l, 34.

Lipton, Stephen M,, and Steven M. Matyas, "Making The Digital Signature Legal--and Safeguarded," Data Communications, Febi;-uary 1978, pp. 41-52.

Little, Arthur D., Inc., "The Consequences of Electronic Funds Transfer: A Technology Assessment of Movement Toward a Less Cash/Less Check Society," NSF Contract C844, June 1975.

Martin, James, The Wired Society, Prentice-Hall, Englewood Cliffs, NJ, 1978.

Marshall, Eliot, "Math Center Protests Army Contract Terms," Science, June 6, 1980, pp. 1122-1123.

Merkhofer, Miley W., Steven B. Engle, and Charles C. Wood, "Decision Analysis Applied to a Technology Assessment of Public Key Cryptographic Systems," 1980 American Society for Engineering Education Conference Proceedings.

Merkle, Ralph c., "Secure Communications Over Insecure Channels," Communications of the ACM, April 1978, pp. 294-299.

Meyer, Carl H., and Walter L. Tuchman, "Putting Data Encryption to Work," Mini-Micro Systems, October 1978, pp. 46-52.

Morgan, Barrie D., and William E. Smith, "Data Encryption: The High Cost of Installing a $50 Chip," Data Communications, February 1977, pp. 25-28.

Morris, Robert, "The Data Encryption Standard--Retrospective and Prospects," IEEE, November 1978, pp, 11-14,

Needham, Roger M. and Michael D, Schroeder, "Using Encryption for Authentication in Large Networks of Computers," Communications of the ACM, December 1978, pp. 993-999.

"The New Money--Promises and Pitfalls of Electronic Funds Transfer," Consumer Reports, June 1978, pp. 354-357.

Nolan, Richard L,, "Managing the Crisis in Data Processing," Harvard Business Review, March-April 1979, pp, 115-126,

Orceyre, M. J., and R, M. Heller, "An Approach to Secure Voice Communication Based on The Data Encryption Standard," IEEE, November 1978, pp. 41-50.

Pantages, Angeline, "Is the World Building Data Barriers?" Datatnation, December 1977, pp. 90-91, 98, 103.

"Privacy and Security in Computer Systems," Institute for Computer Sciences and Technology, National Bureau of Standards, February 1974.

"Privacy Protection--The President's Proposals," Office of Media Liaison, The White House Press Office, April 2, 1979.

"Report of the Public Cryptography Study Group," prepared for the American Council on Education, February 7, 1981.

Rivest, Ronald L., "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," Memo for Scientific American, April 1977.

Rivest, Ronald, Adi Shamir, and Len Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," Laboratory for Computer Science, MIT, Technical Memo 82, April 1977.

Rose, Sanford, "The Unexpected Fallout From Electronic Banking," Fortune, April 24, 1978, pp. 82-86.

Sanders, Sylvia, "Data Privacy: What Washington Doesn .. t Want You To Know," Reason, January 1981, pp 24-37.

Safirstein, Peter, "How Do We Best Control the Flow of Electronic Information Across Sovereign Borders?" AFIPS 1979 National Computer Conference Proceedings, Vol. 48, pp. 279-282.

Schlick, Blair C., "Privacy--the Next Big Issue in EFT," Banking, (no date on copy), pp. 71-76.

Shapley, Deborah, and Gina Bari Kolata, "Cryptology: Scientists Puzzle Over Threats to Open Research, Publication," Science, September 30, 1977, pp. 1345-1349.

Shapley, Deborah, "DOD Vacillates on Wisconsin Cryptography Work," Science, July 14, 1978, p. 141.

"The Spreading Danger of Computer Crime," Business Week, April 20, 1981, pp. 86-92.

Solomon, Richard J., "The Encryption Controversy," Mini-Micro Systems, February 1978, pp. 22-26.

"Starting to Protect Privacy," New York Times, April 10, 1979.

Steen, Arthur Lynn, "Linear Programming: Solid New Algorithm," Science News, October 6, 1979, pp. 234-236.

Sturges, Gerald D., "Summary: Invention Secrecy Act of 1951," - Appendix A to White Paper: Analysis of National Policy Options for Cryptography, U.S. Department of Commerce, National Telecommunications and Information Admenistration, October 29, 1980.

Sugarman, Robert, "On Foiling Computer Crime," IEEE, July 1979, pp. 31-41.

Sykes, David J., "Protecting Data by Encryption," Datamation, August 1976, pp. 81-85.

Tajelski, Tom, "Data Encryption Standard Causes Senate Concern," Security Management, January 1979, pp. 22-23.

"An Uncrackable Code?" Time, July 3, 1978, p. 55.

Appendix A

CONTACTS

This contacts list is divided into two parts. Part 1 lists those individuals interviewed concerning a wide range of cryptography issues to the degree theyfelt able to reply. Part 2 lists those individuals interviewed on the more narrow topic of thefuture of nonmilitary cryptography and its applications.

Part 1

M. M. (John) Atalla, President, Atalla Technovations, Sunnyvale, CA

John Boyle, Vice President/Finance, Crocker National Ba k, San Francisco, CA

Art Bushkin, Sr., Policy analyst, NTIA, Washington, DC

Herbert Chang, Bank of America, San Francisco, CA

David L. Chaum, Ph,D candidate, dissertation on cryptography, University of California, Berkeley, CA

Ronald Clark, Cryptography user, Interbank Research, London, England

Howard Crumb, New York City Federal Reserve Bank, New York, NY

Kent Curtis, Project Administrator, NSF Mathematics and Computer Science Division, Washington, DC

Donald Davies, Cryptography researcher, U.K. National Physical Laboratory, Teddington, Middlesex, U.K.

Whitfield Diffie, Cryptography research scientist, Bell Northern Labs of Canada, Palo Alto, CA

Frank Fojtik, VISA, San Francisco, CA

Leslie Goldberg, Computer security consultant, London, England

Robert Gorman, Cryptography salesman, Racal-Milgo, London, England

Carl Hammer, Senior Scientist, Sperry UNIVAC, Washington, DC

Noel M. Herbst, IBM, White Plains, NY

Lance Hoffman, Professor of Computer Science
George Washington University, Washington, DC

Seymour Jeffery, NBS Computer Sciences Division, Washington, DC

Steven Kent, Research Fellow, MIT-Lab for Computer Science,
Cambridge, MA

Don Kraft, NTIA, Washington, DC

Stephen M. Matyas, IBM, Kingston, NY

Max Meth, Institutional Information Group, London, England

Carl Meyer, IBM, White Plains, NY

Eric Michaelman, SPI Data Systems, Palo Alto, CA

Granger Morgan, Professor, Carnegie-Mellon University, Pittsburgh, PA

Matthew Nimetz, Undersecretary for Security Assistance,
Science & Technology Group, State Dept., Washington, DC

John Oseas, Manager of cryptographic product marketing
IBM, Poughkeepsie, NY

John Pasta, NSF Mathematics and Computer Science Division
Washington, DC

John Pemperton, Cryptograghic product marketer
Communication Security Ltd., London, England

Gerald Popek, Professor of Computer Science, UCLA

Karl Rihaczek, Ph.D., Hamburg, Republic of Germany

Eli Schutzman, Project Administrator, NSF, Engineering Division
Washington, DC

Adi Shamir, Professor, MIT-Lab for Computer Science, Cambridge, MA

Marvin Sirbu, Jr., Professor, MIT-Center for Policy Alternatives
Cambridge, MA

Gerald Sturges, Professional Staff Member, House Subcommittee on Government Information and Individual Rights, Washington, DC

M. N. Sugarhood, Barclay's Bank, London, England

Eli Schutzman, Project Administrator, NSF Engineering Division Washington, DC

Bruce Walker, Ph.D candidate, dissertation on cryptography, Computer Science Department, UCLA

Steve Walker, Information Scientist, DoD ARPANET, Washington, DC

George H. Warfel, Identification Technologies Consultant Financial Service, Menlo Park, CA

Laura A. Weatherly, Manager, Technical Support Services Interbank Card Assoc., New York, NY

Terry N. Westgate, Mount Allison Univ., Sackville, New Brunswick, Canada

Howard Zeidler, VISA, San Mateo, CA

Part 2

Bob Abbott, President, EDP Audit Controls, Oakland, CA

Len Adleman, Professor of Computer Science, UCLA

George Batejan, Chase Manhattan Bank, New York, NY

Al Bayse, Federal Bureau of investigation, U.S. Dept. of Justice
Washington, DC

Dennis Branstad, Senior Scientist, NBS, Washington, DC

Herbert Bright, President, Computation Planning Corporation
Washington, DC

Peter Browne, President, Computer Resource Controls, Washington, DC

Robert Courtney, Computer Security Consultant, IBM, White Plains, NY

George I. Davida, Associate Professor of Electrical Engineering
and Computer Science, University of Wisconsin, Madison, WI

Richard Davis, Mountain View, CA

Harry DeMaio, Director of Data Security Programs, !BM, Armark, NY

Phillip Farley, Visiting Scholar, Stanford Arms Control Research Project
Stanford University, Stanford, CA

Mark Freundel, Research Manager, CRC Systems, Washington, DC

Blake Greenlee, V.P. of Computer Security, Citibank, New York, NY

Herb Grosch, Independent computer security consultant

William Halpin, Vice President, Bankwire Marketing
Payment and Tel.Services, New York, NY

Peter Hamilton, Chubb & Company, London, England.

Martin E. Hellman, Associate Professor Electrical Engineering
Stanford University, Stanford, CA

Vico E. Henriques, President, Computer and Business Equipment
Manufacturers Association, Washington, DC

Ed Jacks, Director of Security, General Motors, Detroit, MI

Robert V. Jacobson, President, International Security Technology

G. Patrick Johnson, Senior Policy Analyst, National Science Foundation Washington, DC

Leo H. Jones, Saber Laboratories, San Francisco, CA

David Kahn, Author, Washington, DC

John Kennedy, Scientists Institute for Public Information, New York, NY

Steve Kent, Ph.D. candidate/consultant, Massachusetts Institute of Technology, Cambridge, MA

Thomas Maril, President, Computer Corporation of America Cambridge, MA

Jeffrey A. Meldman, Massachusetts Institute of Technology, Cambridge, MA

Joshua Menkes, Group Leader, National Science Foundation Technology Assessment and Risk Analysis Washington, DC

Arthur Miller, Professor, Harvard University Law School Cambridge, MA

Donald G. Miller, Assistant Vice President in charge of EDP security The First National Bank of Chicago, Chicago, IL

Ron Rivest, Professor of Computer Science, MIT-Lab for Computer Science Cambridge, MA

Nicholas Schklair, Product Manager, Rocal-Milgo, Miami, FL

Michael D. Schroeder, Xerox Palo Alto Research Center, Palo Alto, CA

Henry D. Taylor, Jr., Marketing Administrative Systems Manager Hewlett-Packard, Palo Alto, CA

Sidney Weinstein, Executive Director, Association for Computing Machinery, New York

Appendix B

CONFERENCE ON FEDERAL GOVER,.NMENT POLICIES
FOR PRIVATE SECTOR CRYPTOGRAPHIC RESEARCH
July 11, 1980

Attendees:

Dennis Branstad
National Bureau of Standards
Washington,DC

Herb Bright
Computation Planning
7840 Aberdeen Road
Bethesda,MD20014

Harry DeMaio
IBM Corporation
Old Orchard Road
Armonk,NY 10504

Phil Farley
Arms Control & Disarmament Project
Stanford University, Building 160
Stanford, CA 94305

Blake Greenlee
Computer Security Department
Citibank
111 WallStreet
New York,NY 10005

Marty Hellman
Dept. of Electrical £ngineering
Durand Bldg.,Room 135
Stanford University
Stanford, CA 94305

Susan Nycum
Chickering & Gregory
3 Embarcadero Center
San Francisco, CA 94111

Gerald Popek
Computer Science Department
University of California
Los Angeles, CA 90024

Ronald Rivest
Computer Science Department
MIT-Lab for Computer Science
545 Tech Square
Cambridge, MA

Nick Schklair
Racal-Milgo
8600 N.w. 41st Street
Miami, FL 33166

Terry Westgate
Mt. Allison University
Sackville, New Brunswick
Canada EOA 3CO

SRI International participants and observers:

Donn Parker
Victor Walling
Charles Wood
Peter Schwartz
Thomas Mandel
Thomas Thomas
David Brandin
David Elliot

From the National Telecommunications Information Administration:

Charles Wilk
Fredrick Weingarten

Appendix C

SRI STAFF INTERVIEWED

Milton Adams, Manager of the Digital Development Group

Craig Blackman, Program Manager, Telecommunications

David Brandin, Exec. Director, Computer Science and Technology Division

George Byrne, Senior Research Engineer

Russell Dewey, Management Systems Consultant

Dave Elliott, Exec. Director, Systems Research and Analysis Division

Bernard Elspas, Staff Scientist

Steve Engle, Decision Analysis Intern

Elaine Hatfield, Research Engineer

E. M. Kinderman, Manager, Nuclear Systems

Termpool Kovattana, Senior Research Engineer

Thomas Mandel, Senior Policy Analyst

Lee Merkhofer, Principal Investigator, NSF Cryptography Project

Peter Neumann, Program Manager

Norm Nielsen, Program Manager

Donald Nielson, Director Telecommunications Sciences Center

John Pickens, Senior Research Engineer

Dean Robinson, Manager, Computer Security Program

Raphael Rom, Senior Research Engineer

Dennis Sachs, Senior Policy Analyst

Peter Schwartz, Senior Policy Analyst

Donn Seeley, Senior Consultant

Thomas Thomas, Director, Center For The Study of Social Policy

Willard Tiffany, Senior Systems Analyst

Douglas Webb, Management Systems Consultant

Harold Winslow, Senior Legal Analyst

James Young, Senior Research Engineer

Appendix D
CURRENT POLICY SITUATION

Policy Element	Status Quo--Major Points
DoD funding role	Major part of all cryptography research is funded by DARPA. This allows DoD to directly influence both the nature of this research and dissemination of the research results. DoD also exercises review authority over NSF-funded contracts.
DoD/NSA review of research results	Nonexistent for projects that are not funded by DoD. Informal control exercised on a contract-by-contract basis when DoD funds projects. No mechanism to screen cryptography papers/speeches for sensitivity is presently operational. 'Meyer letter' demonstrated lack of objective measures for judging the national defense sensitivity of any particular research results.
Export Controls	!TAR regt.lations and munitions control newsletters pr,vide hazy guidance as to the export status of cryptographic hardware, firmware, software, and related technical documentation. NSA participates in the decisions on exportability and assists manufacturers to alter their products so tha they are exportable.
Patent Secrecy	Patent Secrecy Act. NSA participates in decisions on the imposition of patent secrecy orders. The basis for classification of a cryptographic invention as secret is not generally known (of necessity). Inventors are reportedly compensated for their idea.
Research Project Security	Security is generally tighi for projects that are classified but rather lax for those that are not. For unclassified projects, there are no formal restraints on participation in meetings and conferences, on the employment of

foreign nationals, or on travel and the like.

Standardization	Government basically takes the stance that the DES will encourage cryptography use by simplifying interconnection of devices and systems, by lowering the cost of encryption devices, and by being sufficiently strong (at least for the short run). There have been a number of negative reactions to the DES, which, for the most part, claim that the 56-bit key provides inadequate protection. Some claim that U.S. domestic and foreign demand for DES devices has been unduly lowered by rumors that NSA can crack the DES. The DES currently specifies only an algorithm--not a means for integrating cryptography computer information/communication systems. The major advantage gained by the non-DoD sector, in terms of standardization, has been the elimination of the need for those considering implementation of cryptography to actually engage in cryptanalysis.
Regulations for civilian use	Nontechnical regulations for civilian use have mostly taken the form of general directives, such as Regulation E (banking), the Foreign Corrupt Practices Act, and the Privacy Act of 1974. Because the DES is the only commercially available system, they imply its use. Management has the primary responsibility for the evaluation of internal controls and for the implementation of "appropriate" security measures.
GSA Procurement Policy	OMB directives imply, if they do not explicitly dictate, the use of DES equipment. For instance, the DES has been cited in Privacy Act implementation guidelines. As the ratio of the dollar value of cryptography devices purchased by the nongovernment sector to the value of devices purchased by the government increases, the impact of this policy is expected to diminish; it is included because the government remains a major consumer of cryptography products.
Security Certification	In conjunction with NSA, NBS has developed a DES testing procedure that is currently being applied to cryptography devices. The test essentially says "yes" or "no"--the device "correctly" or "incorrectly" carries out the

	DES transformation of plaintext to ciphertext and vice versa. Implementation certification (for protocols and the like) is expected to be available soon.
Other Agency (non-DoD) Funding	Low dollar level projects are funded by DOE, NSF, and NBS. Some of these agencies deal with NSA in a formal way; others do not.
Government Technical Assistance	NSA provides some assistance to private industry researchers working on crypto product R&D. This consists primarily of approval or disapproval of the results reached by the researchers. NBS has issued several publications dealing with the DES and its implementation.
Education of Non-DoD Researchers	A few periodicals, such as CRYPTOLOGIA, deal with cryptographic matters. Several private "road-show" seminars are presented throughout the country. A small number of universities offer cryptography or cryptanalysis courses. Discussion at conferences and meetings proceeds typically without government intervention.
Research Alternatives to Cryptography	A low funding level addresses computer/ communications security in general terms. No projects that deal explicitly with alternatives to cryptography have come to our attention •

Appendix E
APPLICABLE LEGISLATION AND REGULATION

Arms Export Control Act(22 USC 2778) -- authorizes the President to compile a U.S. munitions list.

Atomic Energy Act of1954 (42 USC 2161;43 FR 28950).

Brooks Act of 1965 (P.L. 89-306)--gave NBS responsibility to create standards which would govern the use ofcomputers for federal government. This, in conjunction with the Privacy Act of 1974, caused NBS to issue the DES.

Privacy Act of 1974--attempt to keepconfidential and secure all data on United States citizens which is in possession of the government.

Munitions Control Act of 1954 (now Arms Export Control Act)--to regulate the flow of weapons,computers, and other equipment to other countries.

Office of Management and Budget Circular A-71 -- specifies computer and privacy controls required within the federal civilian government.

Office of Management and Budget Circular A-119 -- provides authority for federal government participation in selected voluntary technical standards development efforts.

International Traffic in Arms Regulations (!TAR), 22 CFR 121-128--permits government to prevent export ofcrypto equipment and crypto technical information. Meansby which the State Department implements provisions·of the Arms Export Control Act.

Inventions Secrecy Act of 1951 --permits Commissioner of Patents and Trademarks to impose secrecy order on aninvention submitted for patent when publicdisclosure could be detrimental to national security.

35 USC 181 -- permits the imposition of secrecy· orders on patent applications when issuance ofa public patent would be detrimental to the national security.

Mutual Security Act of 1954, Section 414-22 USC,1934

Foreign Corrupt Practices Act of 1976 -- asserts that management is required to keep adequate systems of transaction controls,

Foreign Intelligence Surveillance Act of 1978--places restrictions on NSA activities,

42 USC 2274-77, 18 USC 798, 18 USC 952

Executive Order 12036 (June 28, 1978; 43 FR 28949), as amended by Executive Order No, 12148 (July 20, 1979; 44 FR 43239) and by Executive Order 12163 (September 29, 1979; 44 FR 56673)--reguarding national security act and classification,

National Security Act of 1947 and amending Executive Order 11905 (dated 2-18-76)--discuss R&D and use of cryptographic products,

Executive Order 11905--Amends National Security Act of 1947.

White House National Telecommunications Protection Policy Directive (Feb, 15, 1979)--divides messages into three categories and specifies safeguards for each,

Export Control Act of 1949 -- Gave responsibility to the Department of Commerce to control export of technical data and products. The act was renewed in 1951, 1953, 1956, 1958, 1960, 1962, and 1965. Replaced by Export Administration Act of 1969.

Export Administration Act of 1969--legislation dealing with the export of computer networks and their associated building blocks, Encryption devices are explicitly excluded by ITAR. Export Administration Regulations implement this legislation. Amended in 1972, 1974, 1977 and superceded by the Export Administration Act of 1979.

Export Administration Act of 1979--Uses a critical technology approach to the control of exports,

General Services Administration - Federal Property Management Regulation 101-35 -- directs Federal agencies to protect data in their possession,

Appendix F

RISK ANALYSIS AND THE ROLE OF ENCRYPTION

Risk analysis is a somewhat subjective procedure for identifying the most threatening vulnerabilities faced by a particular computer system. This procedure involves:

- Determination of the value to the organization of material data processing assets, including information.
- Identification of threats to these assets.
- Estimation of possible dollar losses associated with each threat.
- Estimation of the probability that each threat will occur within a certain time frame.
- Calculation of the expected dollar loss for each threat, by multiplying dollars times probabilities.
- Ranking of the identified threats by expected dollar loss.
- Selection of cost-effective computer security controls that address the threat with the greatest expected dollar loss.
- Working down the list of threats, selecting controls that provide the most security for the least cost, until an acceptable risk level (or firm budget constraint) is reached.

Vulnerabilities of Computer Systems by Incidence of Loss

SRI's Computer Security Program has for a decade collected information on reported cases of computer abuse. The data base currently contains over 700 cases. An analysis of this data base reveals that the following areas account for the stated percentages of the cases:

Rank	Vulnerability Area*	Frequency**(%)
1	Physical access to facilities (stealing of computer equipment)	25
2	Handling of input data (entering false amounts on input documents)	23
3	Logical access to assets (modifying confidential files stored in the computer)	15
4	Business ethics (simulating the activities of an insurance firm to perpetrate a fraud involving accounting data)	8
5	Handling of output data (stealing checks printed by a computer)	8
6	Access to applications programs (modification of programs which do payroll calculations)	7
7	Handling of machine readable data (replacement of one computer disk pack by another)	7
8	Access to systems programs (modification of login routines so that certain users are no longer able to access the computer. system)	3
9	Backup and recovery (purposely shutting off power to the computer to cause it to crash)	2
10	Data communications (wiretapping)	1

---

* Examples appear in parentheses.
** Total does not equal 100% because of rounding.

Expected Losses Ranked by Threat for an Illustrative Computer System

Listed below from most severe to least severe are the threats faced by one computer system. It is important to note that the ranking, and the terms used to classify threats, will be likely to change from computer system to computer system.

- o Malfunctions and human errors
- o Fraud
- o Power and communications failures

- Fire
- Sabotage and riot
- Other natural disasters
- Other hazards (such as wiretapping)

This list was extracted from Burch, John G., and Joseph L. Sandinas, Jr., Computer Control and Audit A Total Systems Approach, John Wiley and Sons, 1979.

Another Ranking of Threats

Using a different classification scheme, Bob Courtney of IBM has come to the conclusion that the greatest expected dollar losses are to be incurred in these areas (from most to least):

- Errors and ommissions
- Dishonest employees
- Fire
- Disgruntled employees
- Water
- Other threats

These comments have been extracted from a talk that Mr. Courtney gave at an IBM Data Security Seminar, in November 1980.

Examples of Ways to Address These Vulnerabilities

Listed below are only some of the computer security controls and countermeasures that could be used to address the vulnerability areas set forth above.

Physical access to Facilities:
Door locks, gates, guards.

Handling of input data:
Programmed checks to verify that the data submitted to the computer are reasonable, preventing batches of data from being used as input if the sum of each transaction doesn't sum to the batch

control total.

Logical access to assets:
Passwords, allowing only certain users to access sensitive files,

Business ethics:
Adoption of a code of ethics, reporting of suspicious behavior,

Handling of output data:
Placing computer output in locked containers, destruction of output after it has served its purpose,

Access to applications programs:
Establishment of a production set of programs to which changes may not be made unless formal approval is obtained,

Handling of machine-readable data:
Establishment of a library procedure for the use of magnetic tapes.

Access to systems programs:
Passwords, renaming potentially destructive programs, placing systems programs in hardware instead of software.

Backup and recovery:
Keeping a current copy of critical programs stored at a remote site, providing batteries to continue operation in the event that power is no longer available.

Data communications:
Routing of messages through private rather than public networks, and encryption.

Vulnerability Areas That Encryption Can Now Address

Although traditionally many believe that wiretapping is the only vulnerability that encryption addresses, other vulnerabilities may also be handled by encryption. For instance:

- Losical access to resources may be restricted using encryption generated digital signatures as passwords, perhaps preventing unauthotized persons or devices from using system resources.

- Access to application programs may be restricted, again by using digital signatures, but also by encrypting the programs.

- The secure handling of machine-readable data may be augmented if the data are encrypted.

- Access to systems programs, like access to application

programs, may he in part restricted by digital signatures and encryption of che programs themselves.

- Data communications maye carried out more smoothly with the error detection facilities available with several encryption protocols. And, of course, active and passive wiretapping maybe defeated wh$n encryption is used.

Because encryption can address a wide range of threats, it may be more cost-effective than other computer security controls that provide protection from only a small number of threats.

NewThreats Introduced By Use of Encryption

Selection of a computer security control mayinvolve the introduction of new threats. Whenencryption is used, these threats maybe introduced:

- Loss of cryptographic keys - this mayresult in loss of data and backup and recovery problems(if current keys or even cryptographic facilities are not provided by backup systems).

- Theft of cryptographic keys - the thief might be able to ransom the key because data in storage are inaccessible without a certain cyptographic key.

- Malfunction of cryptographic devices, such that encryption or decryption is done using an algorithm or key other than the proper algorithm or key - this may result in lost data, especially if a communication goes in one direction only.

- Failure of cryptographic devices - this does not necessarily result in lost data, but mayhamper operations and expose data to other threats, such as wiretapping.

- Erroneous generation of keys - this situation does not affect the computer system security or operations unless the key generated is one of the very unusual "weak keys."

- Failure to load new keys at proper times - this lessens system security, and maydisrupt operations if other parts of the system haveloaded keys on schedule, but otherwise has no noticeable effect.

- Cryptographic devices mayhave undocumentedcharacteristics - e.g., the cryptographic key could be obtained as output if a stream of zeros was provided as input.

AppenQiX G

PRELIMINARYLIST OF FEDERAL POLICY OPTIONS TO REGULATE ACADEMIC AND COMMERCIAL SECTOR ENCRYPTION RESEARCHANDDEVELOPMENT

Policies to directly regulate cryptographic R&D

Encouragement of licensing of individuals or organizations who engage in cryptographic research.

Security clearance for researchers.

Classification of research on encryption.

Encouragement oflicensing of individuals or organizations who engage in research directly related to encryption, such as certain branches of mathematicsor computer science.

Tracking movement of identified cryptography experts.

Restrictions on patents and copyrights for results of encryption R&D (e.g., secrecy orders).

Restrictions on (or requirements for) publication of encryption R&D results.

Monitoring and investigation of current research.

Limiting encryption research to federally secured locations.

Federal research funding.

Change research proposalapproval process.

Federal education and training of researchers and users.

Issue statements regarding permittedcircumstances for crypto research.

Participation, attendance, and hosting of conferences.

Limiting or requiring the sharing of cryptographic R&D information.

Provide investment tax credit (or other financial incentives) for cryptographic research.

Federal hiring practices (for people doing highly specialized work).

Restrict certain or all foreign nationals from performing cryptographic or cryptographic-related research.

Policies to regulate the use of the products of encryption R&D and thereby alter the incentives for private-sector support of encryption R&D

Certification of products.

Regulation of the application of encryption (such as British constraints on data flow of encrypted information through the telephone and telegraph system).

Encouragement or licensing of individuals and organizations to install or use encryption or encryption equipment.

Federal standard setting and timing of both revisions and new standards.

Continue or modify ITAR (International Traffic in Arms Regulations).

Judicial precedents regarding court access to keys, encrypted data, and also use of encryption methods (1st and 5th amendments).

Regulation of the types of algorithms or keys that may be used [e.g., allow use of Data Encryption Standard (DES) but restrict use of Public Key Codes (PKC)].

Regulation of the types of data that may or must be encrypted.

Policies to alter the need for encryption by end users and thereby reduce the incentives to support encryption R&D

Stiffer legal penalties for violation of nonencrypted data bases and telecommunication systems. (This might be effective protection only for relatively low-unit-value material such as average electronic mail or the Home Box Office type of subscription television.)

Government procurement to alter demand for various types of encryption technology.

New penalties for theft of cryptographic keys or other violations of key management systems.

Limits on the type of information and circumstance in which encryption may be used for data storage or telecommunications.

Policies to alter the need for encryption in international business and commerce

International agreements and treaties to protect transborder data flows in ways that do not require encryption.

International agreements to standardize encryption procedures in computer data storage and telecommunications and thereby reduce reliance on advances in encryption to generate relative advantage in international trade.

Appendix H

POLICY IMPACTS

Three types of impact of each selected policy option are presented:

- o The degree to which the policy could be expected to be feasible and effective in achieving its intended impact.
- o The principal direct but unintended side effects.
- o Probable important indirect effects .

Only selected major impacts have been identified.

The policies analyzed are presented here in five groups:

(1) Policies aimed at altering the rate or direction of nonmilitary cryptographic research directly by altering:
- o The amount of funding.
- o The channels of funding (DoD versus other).
- o The type of research organization funded.
- o The prepublication review requirements.
- o Patent or copyright restrictions .
- o The availability of highly skilled labor.
- o The size and type of the ultimate market.
- o The cost of research and development activity.

(2) Policies aimed at altering the foreign distribution and use of U.S. cryptography by altering:

- o Export controls on hardware.
- o Export controls on technical data.
- o International standards concerning the technical quality of security in electronic systems.
- o International standards concerning application requirements for crypto in electronic systems.

(3) Policies for altering the rate or direction of nonmilitary cryptograghic product development by altering:

- o Product licensing and testing requirements.
- o Invention secrecy requirements.
- o Specifications concerning the applicability or use of the product.

(4) Policies for altering the level of domestic distribution and use of cryptography products by altering:

- o Domestic standards concerning electronic system integrity.
- o Required characteristics of systems to be purchased or used by federal civilian agencies.
- o Required characteristics to assure domestic provision of civil rights, the right to privacy, "due care," and others.

(5) Policies for altering the amount of domestic publicity about cryptography by altering:

- o The government's media profile concerning cryptography.
- o The type and degree of communication between DoD and the nonmilitary cryptography community.

1. Policies for Altering Cryptographic Research Activity

a. Option 1: Reducing/Increasing Nonmilitary Spending For Cryptographic Research

Direct intended impact:

- o Will reduce/increase the number of nonmilitary researchers overtly engaged in cryptographic research.
- o May not alter the rate of new product development in the short run but will probably slow/speed up domestic new product development in the long run.

Direct unintended impacts:

- o Will increase/reduce the dependence of the nonmilitary sector DoD for technical assistance to maintain systems integrity.

- Will reduce/increase the pool of national expertise in cryptology on which DoDor the private sector could draw as needed.

Indirect impacts:

- Will cause both overt and covert shifts in research topics
- Will shift the relative roles of research institutions (large corporate versus public academic; domestic versus U.S. overseas versus foreign).
- Will alter the knowledge basefor nonmilitary security systems design and integrity design.
- May alter progress in related sciences.
- May increase the public debate over cryptography at least in the short run.

b. Option 2: Channeling All Federal Cryptologic Research Support Through DoD

Direct impacts:
- Increased centralization of all electronic systems security research in DoD.
- Increased focus of nonmilitary research on military as well as civilian characteristics.
- Reduced research for civilian needs.

Direct unintended impacts:
- Pullback from overt cryptographic research by some researchers and institutions.

Indirect impacts:
- Increased public attention on DoD as the source of system security.

c. Option 3: Limiting the Types of Organizations Funded to do Nonmilitary Cryptographic Research

Direct Impacts:
- Reduction in the number ofresearchers and amount of academic activity in cryptography.
- Increased separation of cryptography from other topics in system integrity research.

Direct unintended impacts:
- o Reduction in the numberof types of approaches to designing nonmilitary systems using cryptography.

Indirect impacts:
- o Increased reliance by world civilian markets on foreign system integrity research.

d. Option 4: Instituting Voluntary Prepublication Review Process for Nonmilitary Cryptographic Research

Direct impacts:
- o May reduce or redirect some research on cryptography.
- o Will help the defense community staymost current in nonmilitary state of the art.
- o May lead to increased rate of classification of research results.
- o May lead to restrictions on types of research funded.
- o May cause some institutions to discourage cryptographic research projects or to reduce funding for them.
- o May reduce incentive to publish.

Direct unintended impacts:
- o Will continually resurrect the issue of academic freedom (just as the Atomic Secrets Act now does).
- o May alte,: the quality and scope of the basic knowledge base of nonmilitary system integrity product development.

Indirect impacts:
- o May alter the balance of involvement by the defense establishment in other related areas of science.
- o May create more incidents for public discussion.
- o May promptchallenges of the process on constitutional grounds.

e. Option 5: Reducing/ Increasing the Availability of Skilled Cryptography Labor

Direct impacts:
- o Increases / reduces the ability of U.S. institutions to analyze and take protective actions concerning their security and asset protection requirements.

Direct unintended impa[illegible]ts:
- o May reduce the quanity and quality of the overall labor pool for use by the military as well as nonmilitary sectors.

Indirect impacts:
- o Reduced/increased reliance of U.S. firms on foreign technical labor pools

f. Option 6: Limiting/Expanding the Size and Types of Markets for Cryptographic Products (e.g. Through GSA Specifications of Technical or Behavorial Standards)

Direct impacts:
- o Reduced/increased rate of cryptographic sales and application in the short run.

Direct unintended impacts:
- o May move the U.S. cryptography market away from/toward international market trends.

Indirect impacts:
- o Will alter the type and degree of confidentiality and privacy available for both civilian government and private sector files and communication.

2. Policies for Altering Foreign Distribution and Use of U.S. Cryptology

a. Option 7: Reducing/Increasing Export Limitations on Cryptographic Hardware

Direct Impacts:
- o May increase/reduce the effectiveness of future restraints by encouraging/discouraging foreign nonmilitary cryptographic development.
- o Will not alter the international spread of cryptography from other sources.
- o May reduce/increase acceptance of U.S. cryptographic standards internationally.

Direct unintended impacts:
- o May reduce/increase reliance on U.S. computer or telecommunication products.
- o May reduce/increase foreign reliance on U.S. information service industries.

Indirect impacts:
- o May make the process of defining solutions to transborder data flow problems much more complex, especially if U.S. system integrity strategies diverge from those of other nations.

b. Option 8: Restricting/Freeing Trade in Cryptologic Technical Information

Direct impacts:
- o May slow/speed up the rate of technological transfer into as well as out of the U.S.
- o May be ineffective in blocking transfer if the information is publicly available in the U.S.

Direct unintended impacts:
- o Will increase the tension between the military and academic sectors.

Indirect impacts:
- o May alter international trade in other related information.

c. Option 9: Reducing/Increasing Government Involvement in the Establishment and Application of International Quality Standards for Cryptographic Hardware

Direct impacts:
- o Reduce/increase the rate of growth in international trade information, electronic services, and data management.

Direct unintended impacts:
- o Support or undermine private sector efforts to set international standards.

Indirect impacts:
- o May alter the relative balance between government and voluntary organizations in the full range of electronic security and system integrity issues.

d. Option 10: Decrease/Increase Government Involvement in Establishment of International Standards Concerning the Duty and Care in Providing Security and Asset Protection

Direct impacts:
- o Will alter the rate at which standards of care are established,
- o Will alter the balance between personal and state rights in the standards established

Direct unintended impacts:
- o Will alter the world perception of the U.S. on human rights issues such as free speech and privacy.

Indirect impacts:

- o Will alter the difficulty and likely result of resolutions to some transboarder data flow issues.

3. Policies for Altering the Rate or Direction of Domestic Cyptographic Product Development

a. Option 11: Decreasing/Increasing Licensing and Testing Requirement for Cryptographic Products

Direct impacts:

- o Decrease/increase the cost of developing and marketing a new product.
- o Decrease/increase the minimum market price of a new product.

Direct unintended impacts:

- o Decrease/increase the amount of bureaucracy, and related cost necessary to operate secure private sector electronic systems

Indirect impacts:

- o Create additional bureaucratic processes and costs to the government.

b. Option 12: Reducing or Increasing Use of Invention Secrecy for Cryptography

Direct impacts:

- o Reduces/increases risks of undertaking commercial development of security technology.
- o Will reduce/increase reliance on trade secrets.
- o May reduce/increase reliance on foreign product development.
- o May reduce/increase the quality and type of nonmilitary cryptographic protection available in the U.S.

Direct unintended impacts:

- o Reduces/increases the opportunity and incentive for foreign suppliers to make faster nonmilitary progress in cryptography.

Indirect impacts:

- o Will reduce/increase the competitive incentives for foreign competitors worldwide and toward the U.S. market.
- o May alter the strategies used by corporations to protect property rights in transborder data flows.

c. Option 13: Reduce/Increase Federal Specification of Applications and Uses of Specific Cryptography (Such as DES)

Direct impacts:
- o Will reduce/increase the extent to which cryptography is used in the short run.

Direct unintended impacts:
- o Will increase/reduce the vulnerability of civilian communication and file security.

Indirect impacts:
- o Will alter the relative comparative advantage and attractiveness of U.S. markets to foreign suppliers

4. Policies for AlLer[illegible]ng Domestic Distribution and Use of Cryptography

a. Option 14: Altering Domestic Standards for System Security and Integrity

Direct impacts:
- o Increase/decrease the ease of replacing technology with a new product (e.g. GSA design standards would freeze in a tecl,[illegible]ology while performance standards would permit continual innovation against a behavorial objective).
- o May set defacto standards for some commercial applications (e.g. telephony) shared with civilian government.

Direct unintended impacts:
- o Will increase/decrease susp1c1on of NSA manipulation of civilian cryptographic system strength.

b. Option 15: Alternative Federal Standards for Cryptography Procurement (Commercial Versus Goverment Specifications)

Direct impacts:
- o Reuuce/increase the similarities between the commercial and civilian markets.

Direct unintended impacts:
- o Alter the -[illegible]at[illegible]t which foreign cryptographic equipment is introduc[illegible]d into the U.S. markets.

5. Policies on Domestic Cryptologic Publicity

a. Option 16: Altering the Government Media Profile on the Topic of Cryptology

Direct impacts:
o Lessen/increase public attention to cryptography.

Direct unintended impacts:
o May raise attention to precisely what the national security communitywould like to keep quiet.

Indirect impacts:
o May set dangerousprecedent for news manipulation.

Appendix 1

A FRAMEWORK FOR ASSESSING CRYPTOGRAPHY IN THE NONMILITARY SECTOR OF SOCIETY: THE BROADER ISSUE OF COMPUTER AND COMMUNICATION INTEGRITY

Encryption represents only one safeguard for protecting data from errors and abuse and for facilitating electronic transaction control. In fact, for encryption to be effective requires signiricant safeguarding of keys and key administration. Research in encryption must be considered in the broader context of making computer use, communications, and electronic transactions safer and more efficient.

Research in other computer and communications security (including transaction controls) is as sensitive in many respects as encryption research. For example, research in provably secure computer operating systems is progressing with demonstration of pilot models. Identification verification of terminal operators is also a subject of research leading to a numb[illegible]of Gecurity products. IBM made available a new version of its Resource Access Control Function software package in Europe before selling it in the United Staes. Several commercial access control products are available, and research on more advanced products continues.

It is important that security against intentionally caused losses is strongly determined by the weakest link or greatest vulnerability in a system. The vulnerabilities that encryption is designed to protect against are, it is generally agreed, not necessarily the weakest links, That is, there are usually easier and safer ways for an intruder to accomplish his goals. He may find that stealing a computer output report from an office or compromising a computer program is a more attractive way to obtain data than tapping a phone line, for example.

The options to affect the research and development of encryption are also applicable by extension to all computer and communications security research and development. It is, therefore, reasonable to generalize the options to cover the whole range of the subject. This approach would avoid suboptimization focused on only one of many security issues, accomplish consistent policy over subjects that must also be addressed in any case, and reduce the cost.

An argument against this broad approach might be that it encompasses more than can be practically managed. Therefore, isolating and treating only encryption as a first step would lead

to easier adoption of the broader issues. However, we are not yet convinced of this.

Cryptography in an Expanded Context

When cryptography is put in its proper context both, technologically and according to its need in the public sector, the following ideas emerge.

Cryptography is just one safeguard amongmany importantmeansof making information processing and communicationssafe from errors, omissions,misuse, and abuse and of providing transaction control. It is not worthy of special treatment and in fact cannot be technically or scientifically isolated from other safeguard efforts such as operating system integrity.

The safeguard needs for military and other secret federal government secret activity require a specialized research and development culture, environment, and methodology suchas are found in NSA, which are different from research and development in the public sector, such as in academic institutions and NBS. The former sector can draw freely on the resources and results of the latter, both covertly and overtly, but the reverse can occur only with concurrence and selective release by the secret components of the government.

Information security needs in the U.S. public sector are increasing as the value of information in electronic form increases. As Lhis sector increases its reliance on electronic processing and communication, these needs will becomeso critical that national security concerns will expand to include the security of automated banking and the financial industry, the communications industry, energy distribution and control, transportation, weather prediction and control, and others.

Th&#65533;need for information security in the public sector transcends national borders and interests. Research and development in security, especially that including cryptography, is actively pursued in other countries, so that any drop in level of effort in the United States would have no effect on efforts in other countries. In fact, it would probably encourage such efforts on a competitive basis. In addition, U.S.-based multinational companies havesomeof their greatest information security concerns in foreign communication and information processing activities.

Recommendations

In view of the foregoing conclusions, the following general recommendationsare made. Cryptography should not be isolated and created seperately from other information safeguards. Cryptography

should be treated as an integrated function within information processing and communication systems. In addition, policy should not depend on differentiating between cryptography and other related research topics and not dependent upon differentiating between data processing and data communication functions within an information system.

Summary

The issues concerning cryptography include such subjects as designing, developing, and proving secure computer operating systems, data file access protection mechanisms, communication compromise detection devices, and computerterminal and telephone access identification methods. The thrust of cryptographic research and development will be primarily toward systematizing its use, product implementation, key selection and management and applications rather than toward further algorithm and cryptanalysis discovery. However, a breakthrough in mathematical or electronic sciences could require a return to basic research. Poiicy must anticipate this possibility .

FORM **NTIA-29**
(4·80)

U.S DEPARTMENT OF COMMERCE
NAT'L. TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION

BIBLIOGRAPHIC DATA SHEET

	1 PUBLICATION NO	2. Gov't Accession No.	3. Recipient's Accession No.
4 TITLE AND SUBTITLE IMPACTS OF FEDERAL POLICY OPTIONS FOR NONMILITARY CRYPTOGRAPHY; Research Report 3; April 1981			5. Publication Date
			6. Performing Organization Code
7 AUTHOR(S) Victor C. Walling, Jr. / Donn B Parker; Charles C. Wood			9. Project/Task/Work Unit No.
8 PERFORMING ORGANIZATION NAME AND ADDRESS SRI International 1333 Ravenswood Ave. Menlo Park, California 94025			10. Contract/Grant No.
··· Name and Address COTR: Charles K. Wilk 1325 G Street, N.W. Washington, D.C. 20005			12. Type of Report and Period Covered
			13.

ksueecwrnrna, NOm

ABSTRACT r*A 200-word or less factual summary of most significant 1nformat1on. If document includes a significant bibliography or literature su,vey. mention ,there.)*

A study accomplished by SRI International under contract with the Commerce Dept., NTIA, in support of work toward developing a U.S. policy for cryptography. It provides an analysis of the policy options based on a projection of evolving private sector needs for privacy and security, the emerging potential for innovative applications such as public key cryptographic systems, the influence of government constraints on exports, inventions, research and innovation, scientific advancement, and the preservation of constitutional rights. It 1 recommends a balanced framework for U.S. policy, including minimization of existing restraints on private sector activities concerning exports and patents, governmr:mtsupport of open research and technical standards development, and the establishment of a government mechanism for resolving conflicts between private sector and U.S. military interests.

16 Key Words *(Alpt,abet,cal order. separated by semicolons)*

computer security; cryptography; export controls; International Traffic in Arms Regulations; Inventions Secrecy Act; national policy on cryptography; patent secrecy; privacy; public key cryptography; telecommunications security.

17 A'',',ILABILITY STATEMENT D UNLIMITED D FOR OFFICIAL DISTRIBUTION	18. Security Class. *(Th,s report)* Unclassified	20. Number of pages 99
	19. Security Class. *(This page)*	21 Pnce: