

**Information Security:
An Elusive Goal**

George F. Jelen

Program on Information Resources Policy

Harvard University

Center for Information
Policy Research

Cambridge, Massachusetts

A publication of the Program on Information Resources Policy.

INFORMATION SECURITY: AN ELUSIVE GOAL

George F. Jelen

June 1985, P-85-8

Project Director: Anthony G. Oettinger

The Program on Information Resources Policy is jointly sponsored by Harvard University and the Center for Information Policy Research.

Chairman: Anthony G. Oettinger

Managing Director: John C. LeGates

Executive Director: John F. McLaughlin

Executive Director: Benjamin M. Compaine

Executive Director: Oswald H. Ganley

George F. Jelen wrote this paper as a visiting fellow from the National Security Agency, Department of Defense.

Copyright © 1985 by the Program on Information Resources Policy. Not to be reproduced in any form without written consent from the Program on Information Resources Policy. Harvard University, 200 Aiken, Cambridge, Ma 02138. (617) 495-4114. Printed in the United States of America.

PROGRAM ON INFORMATION RESOURCES POLICY

April 1995

Harvard University

Center for Information Policy Research

Affiliates

AT&T Corp.
Apple Computer, Inc.
Applied Telecommunications Technologies,
Inc.
BellSouth Corp.
Braxton Associates
Carvajal S.A., Columbia
Centro Studi San Salvador, Telecom Italia
The College Board
Commission of the European Communities
Computer & Communications Industry
Assoc.
CSC Index (England)
CyberMedia Group
DACOM (Korea)
Deloitte & Touche
DRI/McGraw Hill
Educational Testing Service
EG&G, Inc.
ETRI (Korea)
European Parliament
France Telecom
Grupo Clarin (Argentina)
GTE Corp.
Hitachi Research Institute (Japan)
IBM Corp.
International Resource Development, Inc.
Japan Telecom
Knight-Ridder Information, Inc.
KPN (Netherlands)
Lee Enterprises, Inc.
Lincoln Laboratory, MIT
Martin Marietta Corp.
John and Mary R. Markle Foundation
McCaw Cellular Communications, Inc.
MeesPierson (U.K.)
Mead Data Central
Microsoft Corp.
MITRE Corp.
National Telephone Cooperative Assoc.

NEC Corp. (Japan)
The New York Times Co.
Nippon Telegraph & Telephone Corp. (Japan)
North Communications
Northern Telecom
NYNEX
Pacific Bell
Pacific Bell Directory
Pacific Telesis Group
Raytheon Co.
Research Institute of Telecommunications
and Economics (Japan)
Revista Nacional de Telematica (Brazil)
Samara Associates
Scaife Family Charitable Trusts
Scientific-Atlanta, Inc.
Siemens Corp.
Southern California Edison Co.
Sprint Communications Co. L.P.
State of California Public Utilities
Commission
Strategy Assistance Services
Telstra Corp. Ltd. (Australia)
Times Mirror Co.
TRW, Inc.
United States Government:
Department of Commerce
National Telecommunications and
Information Administration
Department of Defense
National Defense University
Department of Health and Human Services
National Library of Medicine
Federal Communications Commission
National Security Agency
U.S. General Accounting Office
U.S. Media Group
Viacom Broadcasting
VideoSoft Solutions, Inc.

Acknowledgments

The author greatly appreciates the cooperation of those who agreed to be interviewed for or quoted in this report:

Robert P. Abbott
James P. Anderson
Howard Barlow
James H. Burrows
Leslie S. Chalmers
James J. Croke
Walter G. Deeley
Harry B. DeMaio
Henry Geller
Bobby R. Inman
William P. King
Donald E. Kraft
Roland O. Laine

Theodore M. P. Lee
Steven B. Lipner
Robert C. Massey
Peter G. Neumann
Harold J. Podell
Roger R. Schell
Robert H. Scherer
James A. Schweitzer
Raymond T. Tate
Stephen T. Walker
Charles K. Wilk
Thomas Witcher
John P. L. Woodward

as well as several others who preferred not to be identified.

Special thanks are also due to the following persons who reviewed and commented on early drafts of this report. These persons and the Program's affiliates are not, however, responsible for or necessarily in agreement with the views expressed herein, nor should they be blamed for any errors of fact or interpretation.

Dana W. Atchley, Jr.
Thomas Bartee
Eugene Bloch
Nancy Carey
John V. Clark
George R. Cotter
James J. Croke
Patrick M. Daly
Harry B. DeMaio
Whitfield Diffie
Gerald P. Dinneen
William C. Ditch
Robert L. Dryden
Hilda Faust Mathieu
Henry Geller
Robert E. Gradle
Sidney J. Green

Jan Herring
Ceil Hlawatsch
David Kahn
William P. King
Donald E. Kraft
Stephen B. Lipner
David J. Markey
Howard E. Rosenblum
Alan E. Schechter
Stephen C. Schmidt
James A. Schweitzer
Peter Schweitzer
Robert Sexton
Raymond T. Tate
Julia B. Wetzel
Ralph T. Whiteside
J. Michael Williams

TABLE OF CONTENTS

	Page
Executive Summary	i
Foreword	iii
PART I -- INTRODUCTION	
Chapter 1. Power vs. Restraint: The Security Dilemma	I-2
Chapter 2. Worlds Apart or Parts of One World?	I-6
Notes	I-18
PART II -- HISTORICAL BACKGROUND	
Chapter 3. The Era of Dependence	II-2
Chapter 4. A Government Monopoly	II-19
Chapter 5. A Challenge to the Monopoly	II-45
Chapter 6. From Task Forces to Kernels to Laws	II-68
Notes	II-93
PART III -- THE CURRENT CONDITION	
Chapter 7. A Confusing Muddle	III-2
Chapter 8. Two Opposing Views	III-32
Chapter 9. Risks, Interests, and Markets	III-60
Notes	III-92
PART IV -- LOOKING AHEAD	
Chapter 10. A Second Look at Strategies	IV-2
Chapter 11. If We Know Where We Want To Go, Why Don't We Get There?	IV-30
Chapter 12. Security vs. Secrecy: In Pursuit of a Balance	IV-61
Notes	IV-68
APPENDICES	
A. "A Plan for the Evaluation of Trusted Computer Systems," draft dated 22 February 1980.	V-2
B. Deputy Secretary of Defense Memorandum, Subject: DOD Computer Security Evaluation Center, dated 2 January 1981.	V-10
C. Department of Defense Directive 5215.1, Subject: Computer Security Evaluation Center, dated 25 October 1982.	V-11
D. National Security Decision Directive 145 (Unclassified Version) "National Policy on Telecommunications and Automated Information Systems Security," dated 17 September 1984.	V-18

EXECUTIVE SUMMARY

The term "information security" describes efforts to protect information in large systems. In addition to physical and administrative controls, it includes communications security (COMSEC) and computer security (COMPUSEC). In modern systems, COMSEC and COMPUSEC are interdependent and often indistinguishable. Yet, for historical, economic, and political reasons, the two are being pursued separately and differently -- particularly within the federal government. Furthermore, the pursuit of information security often leads to a dilemma: the more one tries to protect information, the harder it is to use and the more useable one tries to make the information, the harder it is to maintain security. Because of these and other factors, information may not be getting the protection it should.

When the government discovered a large need for additional COMSEC devices during World War II, it was forced to depend upon industry and independent inventors. Shortly after the end of WWII, however, the government consciously and systematically brought COMSEC development under its own tight control and centralized it in a single Department of Defense (DoD) agency.

In 1977, in response to concerns about personal privacy and foreign eavesdropping, President Carter issued a presidential directive that, in effect, broke up the DoD monopoly. The directive distinguished between national security-related information and that which was not national security related. The first, it left the responsibility of the DoD; the second, it assigned to the Department of Commerce. For a variety of reasons, including a thorny definitional one, this attempted split failed to take, and the Department of Commerce has essentially backed out of the COMSEC business.

Meanwhile, during the late '60s and early '70s, computer security became a government concern, particularly within the DoD and the Intelligence Community. Efforts aimed at technical solutions started in a number of locations. Rather suddenly, in 1976 the major DoD player lost interest in the effort and withdrew its funding, creating a hiatus from which the DoD has had difficulty recovering. In 1981 the DoD decided to focus its computer security efforts by establishing the Computer Security Evaluation Center as an independent organizational entity -- deliberately separate from the DoD's COMSEC effort. To address the COMPUSEC needs of the government's civil agencies, a number of laws were passed but very little was actually done. A major problem has been that no one has been in charge.

Thus, responsibility and authority for information security within the government have been in something of a muddled state, divided along COMSEC-COMPUSEC lines and along national security-civil lines as well. Although a new residential directive represents a positive step, the overall state of information security within the government remains troubling. What progress has occurred has been extremely slow in coming.

There is considerable divergence of opinion regarding how best to proceed. A basic question is whether COMSEC and COMPUSEC should be pursued separately or together. A disagreement over strategy reinforces the argument over separation. COMSECers tend to feel more comfortable with government sponsorship and classified environments. Computer security practitioners, on the other hand, tend to favor industry development and open environments.

Important stakes rest upon the outcome of this debate. The protection of information important to security of the country could be at risk. There are economic interests for those companies that might or might not be able to respond to the stated requirement, depending upon the debate's outcome. Yet in spite of an obvious need for better and more secure products, this market remains weak.

The two competing strategies of government risk-taking combined with a classified environment (traditionally favored by the COMSEC community) and of industry risk-taking combined with an open environment (generally favored by the COMPUSEC community) are not the only strategies possible. Government risk-taking could be combined with an open environment or industry risk-taking with a classified environment. In fact, there are examples where each of these has been successfully employed. So the government would seem to have a choice of four strategies -- not just two. Since each of the four has its attendant advantages, choosing one from among them would be difficult. Fortunately, a choice is not necessary; the government could pursue more than one at a time.

But the government may not have the power and freedom to choose its own strategy. The success of any selected government strategy will be largely determined by the extent of industry cooperation. Presently, the computer industry, the intended source of COMPUSEC products, shows little interest in government sponsorship. The industry also perceives a lack of demand outside of the government. Thus, the prospects for an adequate supply of information security products in the near future appear dim. And without adequate products, the nation's information is likely to remain at risk.

Still, there is a chance that secure products will be developed. If so, their arrival presents greater challenges. The power to protect is equivalent to the power to control, and there are many who would not like to see such power in the hands of the government. At the same time, without any such power, our nation would be exceedingly vulnerable. What is needed, then, is a balance -- a balance between the government's need for secrecy and its citizens' need for privacy and liberty.

FOREWORD

On 17 September 1984, President Reagan signed National Security Decision Directive 145 (NSDD-145) (see Appendix D). NSDD-145 represents a major step by the federal government toward consolidating its efforts to protect information and toward placing computer security on a common policy structure with communications security. NSDD-145 was signed while the draft of this report was out for comment -- long after most of the research for the report had been done. Yet rather than rendering the report obsolete, the signing gives it added relevance.

This report deals with many of the same issues that the directive is intended to address, from those associated with the exigencies of information security to those resulting from the organizational and policy separation that has existed between the communications security and computer security efforts of the government. But the report does more. It also provides a framework for assessing how well the policy is likely to work.

The government's success will largely hinge upon industry's cooperation. But industry may be in no better position to respond to the greater demands placed on it than government policy has been. The new directive is important and controversial. While it is hailed by those who are concerned about the need to secure the government's secrets and personal data, it is at the same time feared by those who resist any trends toward tighter government control, as this step might presage.

PART I

INTRODUCTION

Chapter 1

Power vs. Restraint: The Security Dilemma

Although a trite statement, it is nonetheless true that we are experiencing a technological revolution -- an explosion of knowledge and a geometric expansion of its uses. According to one writer:

We live in an era in which it is technologically possible for every thought, experience, and event to be transmitted, stored and retrieved. It is possible -- technologically -- for everyone to talk to everyone else, to obtain instant and ample knowledge about all things, everywhere on earth.

What technology proclaims to be possible, the marketplace soon declares to be necessary. It is as if whatever technological advance my competition or my neighbor can have, I must have.

Like materials and energy, information is now seen as a basic resource.² As with any other valuable resource, those who have it wish to profit from it. They want to use it, to trade with it, to sell it, and to gain power from it. But they also want to be able to protect it. Herein lies the dilemma.

Nowhere is this dilemma felt more forcibly than in the military and intelligence communities. Speaking for the military side, Major General Robert J. Herres, Commander of the Air Force Communications Service, told a group studying the Air Force's computer security needs and efforts during the summer of 1979:

. . . [I]t seems that we're in some sort of dilemma: on the one hand, we must maintain the security and integrity of our sensitive information, but on the other hand we must be able to respond quickly to rapidly changing situations, especially during times of crisis or war. And this means that we must process and distribute information rapidly

among many people at different levels of command, and possessing a variety of clearances and "needs-to-know."

We cannot let security considerations throttle our operational responsiveness, but we also cannot jeopardize sources of intelligence information, war plans, actions, or sensitive information by having some unknown hole in our security which could be exploited by some individual or group, quite undetectably.³

Dr. John Koehler, Deputy Director for Central Intelligence for Resource Management, made essentially the same point on behalf of the intelligence community:

The Intelligence Community always faces a dilemma: because our sources are fragile, the information needs to be closely held, locked up, protected. But the purpose of gathering and producing intelligence is to help make better decisions. That requires data to be processed⁴ quickly and information disseminated quickly and broadly.

It is clear, then, that to be useful, information must be transportable -- quickly and accurately. A reliable means by which the information may be conveyed or delivered from one location to another must exist. Computers that store the information must be able to exchange their data. Users of one computer, like users of one branch library, want ready access to information residing in another. The communications networks that link these computers must therefore be flexible and reliable, providing redundant paths and permitting real-time rerouting when necessary. But as the utility and functionality of these networks is thus enhanced, their security is correspondingly threatened. ". . . [T]he use of data communications networks in the implementation of information systems has materially increased the vulnerability of data to compromise and unauthorized modification," declared one technical article.⁵ As Carol Bellamy, then President of the New York City Council, pointed out in 1980, "Part of the challenge of the '80s and the '90s and the year 2000 on

is to take the information we have, to make it manageable and be able to function with some, some degree of security with all the information."⁶

To provide this security in the face of the increased vulnerability, security mechanisms are conceived, designed, and built. These security mechanisms must be capable of protecting networks that vary considerably in functionality, complexity, and threat.

To the extent that the networks themselves vary from system to system, so must the mechanisms intended to protect them. In the words of one writer:

Networks span the spectrum from collections of heterogeneous, autonomous host computers to groups of hosts operating under a single authority and cooperating to provide a coherent, supra-computer interface. Correspondingly, the types of measures provided for network security vary over a wide range, depending on the network environment.

However, whatever measures are contrived to protect a given network, they must combine to comprise a single security system. As a technical journal article explains:

Generally security is a system problem. That is, it is rare to find that a single security mechanism or procedure is used in isolation. Instead, several different elements working together usually compose a security system to protect something.

Different elements address different security concerns. Among the security concerns usually listed are physical security, personnel security, communications security, hardware security, software security, and procedural or administrative security.⁹ Of these, physical security, personnel security, and administrative security tend to be externally applied. Solutions to these concerns usually lie outside the physical entity itself and thus tend to be independent

of the particular system they protect. These, although important, are not the principal focus of this study.

In this study we shall discuss the set of security concerns usually addressed within the system, i.e., communications security, hardware security, and software security. Features designed to deal with these concerns characterize the system, and being built in, are less easily changed. Following common practice, hardware and software security will be considered together and referred to as computer security, which Lance J. Hoffman defines as referring "to the technological safeguards and managerial procedures which can be applied to computer hardware, programs and data to assure that organizational assets and individual privacy are protected."¹⁰ In a large teleprocessing network comprising a number of host computers interconnected via a complex array of communications paths, communications security (COMSEC) denotes those measures taken to protect their interconnecting paths; computer security (COMPUSEC) refers to those measures applied to the host processors themselves.¹¹ When combined with the externally applied controls of physical, personnel, and administrative security, COMSEC and COMPUSEC comprise "information security,"¹² which simultaneously acts to protect one's information and to impose restraints on how one may prudently use it, thus limiting its intrinsic power.

Chapter 2

Worlds Apart or Parts of One World?

Giving them different names does not mean that COMSEC and COMPUSEC are really distinct. In fact, they are often totally interdependent.

On the one hand, it has been recognized for several years that computer security in many systems cannot easily be achieved without cryptographic¹³ protection (a form of COMSEC) of the communications links. A working group specifically appointed by the National Communication Security Committee (the former national policy-making organization for COMSEC) to study computer security issues has stated:

Cryptographic protection of communications components of an ADP system is an essential part of system security. In addition to protecting information during transmission, cryptographic techniques have the potential to improve (a) control over electrical access to computer systems, and (b) protection of data or security relevant information stored in the computer.¹⁴

On the other hand, one of the most critical concerns in a cryptographic or COMSEC system is that of key management -- the method used to effect the necessary preexchange of private information to permit successful intercommunication over an encrypted link. The system can never be more secure than the protection afforded the key.¹⁵ In large internettted systems, functional requirements often virtually dictate automatic key distribution, i.e., key distribution performed or controlled by a computer. It is obvious that in such an instance the communications security of the network depends in a very real way on the computer security inherent in the key distribution computer.¹⁶

Not only are COMSEC and COMPUSEC interdependent, they are often indistinguishable. Authentication on a communications line is considered a form of communications security and is usually achieved through cryptographic means. Identification of a user at a computer terminal, however, is usually thought of as part of access control -- a computer security feature. But for all intents and purposes they are one and the same.

This identity at the mechanism level is complemented by an inseparability at the system level. The report of the NCSC Working Group stated:

The boundary line between what is the "computer system" and what is the "network" is at best arbitrary This difficulty in separating functions makes it all the more imperative that computer systems security be approached from a total systems perspective.

The interdependence and the inseparability of COMSEC and COMPUSEC is a direct consequence of the convergence of computers and telecommunications themselves. The advent of computer networks has made previous distinctions obsolete and meaningless. As one recent book on computer networks put it:

Computer networks are derived from a combination of computers and telecommunications -- two technologies with very different histories and traditions

We now have a technological convergence of computers and telecommunications, both sharing the same kind of logic, storage, switching and transmission. Convergence has another meaning, because information handling systems now employ telecommunications and information-processing in such an intimate mixture that we find it difficult to say what is processing and what is communications.

Thus it would seem that any organization intent upon true information security would draw no distinction between COMSEC and COMPUSEC, but pursue them as one. This is not happening. It is even possible that it cannot happen. For despite the technological

evidence that the two are one, other influential factors impose a distinction. So it is that COMSEC and COMPUSEC, in both the public and private sectors, are characterized by separate organizations pursuing separate policies and developing separate mechanisms aimed at separate security standards.

One author has observed:

The organization of American government agencies has tended to mirror, for functional or philosophical reasons, certain separations that are deemed significant, if not semi-sacred: the separation of the domestic from the foreign, the civilian⁹ from the military and the private from the public.

He might well have added "and the world of the computer from that of communications." As a January 1983 editorial in the Electronic News commented, "There are still two distinct worlds polarized around AT&T and IBM" ²⁰

This bipolarity characteristic of the entire information sector is reflected in the field of information security as well. For example, before NSDD-145 the responsibility for setting government policy in information security appears to have been split at least four ways, depending upon whether or not the information is related to national security and upon whether the information is stored within a computer or transmitted over a communications line. ²¹ And in most technical areas, both government and industry pursue COMSEC and COMPUSEC separately.

Not only are the two components of information security being pursued separately, but they are being pursued differently. For example, there are fundamental differences between the way in which the government procures COMSEC devices and the way it is attempting to acquire COMPUSEC mechanisms. As a general rule, in the COMSEC world

the government has borne the risk of development. Also, the COMSEC world has traditionally required that the devices be developed and produced in a classified environment. In the COMPUSEC world, however, the government is asking industry to bear the risk and is favoring open discussions in an unclassified environment.

The reasons for this separateness and these differences are many. Some are historical; some are economic; some are technological; some are political.

Communications security and computer security have profoundly different histories. The two parent industries, communications and computers, developed separately and, not surprisingly, their offspring have as well. COMSEC, like its parent, is much older. The early development of COMSEC devices is closely associated with World Wars I and II -- there was rarely a question of need. Also, COMSEC has traditionally been characterized by tight government restriction enforced through security classification controls. COMPUSEC, on the other hand, is newer. It seems to have had its birth in the late 1960s. Although the Vietnam War was still going on, the impetus for COMPUSEC was not so much the protection of tactical information associated with making today's war as the protection of strategic information associated with making weapons and planning tomorrow's wars. People can and do argue need. Finally, COMPUSEC is and has been characterized by rather free and open exchanges at an unclassified level among government, academe, and industry. Although COMSEC is now more openly discussed, this is a rather recent phenomenon, and very little of this public discussion has anything whatever to do with COMSEC for national security requirements.

Economic considerations have also imposed a distinction between COMSEC and COMPUSEC.

For one thing, the cost-benefit ratios are quite different. For a relatively modest investment in a cryptographic device, the security protection afforded a communications link can be greatly enhanced. To yield a comparable improvement in the internal security of a computer requires a much greater investment. This is not only because COMSEC is a much more mature technology but also because COMPUSEC cannot effectively be added on or appended. It has to be designed in from the beginning,²² a fact that has been clearly and repeatedly demonstrated by abortive attempts to "patch holes" discovered in existing systems.²³

Second, cost savings have been an objective in COMPUSEC but not in COMSEC. Although the sales of COMSEC devices have clearly been affected by price, nothing in the history of communications security suggests that it was pursued for any fundamental reason other than security. Computer security, however, seems always to have had a second basic objective -- to save money. As early as 1972 an Air Force funded study recognized this dual purpose, stating:

The consequences of the inadequate security mechanisms in current Air Force computer systems are both the potential for loss of information critical to national security²⁴ by enemy penetration and a higher cost of operation.

That same report priced these "consequences" at "about \$100,000,000 per year" for the Air Force alone.²⁵

If computer security is to fulfill this second goal, it must be reasonably priced. In particular, it cannot cost more than the physical or administrative controls that are imposed in its absence.

Next, there are technological differences. While it is true that the merging of communications and computer technologies within information systems makes it increasingly difficult to separate COMSEC from COMPUSEC concerns, there are nevertheless two distinct base technologies. These technologies -- cryptology for COMSEC and trusted computing base (TCB) technology for COMPUSEC -- are sufficiently different that there are very few true technical specialists in both. Complicating the issue is the fact that there is no technical reason that cryptology cannot be used to help secure computers nor TCB technology to enhance the security of communications. In fact, both can be and are.

And finally, politics has had a hand in the separation. Political considerations exist at the level of the president and the Congress -- the level of "high politics" -- as well as at the bureau or agency level and below -- the level of "low politics." Most of the significant early development of COMSEC devices took place during an era when government was generally trusted. That of COMPUSEC did not. When COMSEC device technology was maturing, the environment was that of a country unified by war against a common, foreign enemy. The current political environment surrounding the government's efforts in computer security is set against the backdrop of Watergate and the National Data Center scare. The "high politics" factor, then, is that in the minds of many people today, the enemy to be feared most is the government itself. And at the "low politics" level, argument over separation is often hard to distinguish from normal bureaucratic battles over turf.

Probably reflecting a difference in maturity of the two base technologies, COMSEC mechanisms, even for the relatively immature needs of the non-national security sector, are far more abundant than are those for COMPUSEC. A December 1980 report published by the National Telecommunications and Information Administration listed 160 commercially available products (55% of U.S. manufacture) supplied by 32 vendors.²⁶ By contrast, a 1982 computer security conference was able to boast of only a single commercially supported product. A speaker at that conference bemoaned:

. . . the fact is that the need for secure systems for important national defense applications has not been diminished in the slightest²⁷ by any work that has gone on over the past twelve years.

Whether because of or in spite of these seemingly unimpressive results, there are persons, organizations, and institutions who are firmly convinced that the present separation between COMSEC and COMPUSEC must continue -- that if the U.S. is ever to acquire robust computer security mechanisms, it is imperative that the "business" of computer security continue to be conducted separately and differently from that of communications security. Other persons and organizations are equally convinced that so long as mechanisms for computer security and communications security are separately pursued, the security of neither computers nor communications will be adequately achieved. As these two convictions battle for dominance, much could be at stake. Some organizations within government, business, and industry may find themselves in relatively weaker or stronger positions depending upon the outcome. Among others, the following questions arise:

- Does the current separation between COMSEC and COMPUSEC aid or retard the availability of trusted computer security production?
- To what extent might the security of information belonging to government and to business be at risk? Does the current separation between COMSEC and COMPUSEC in any way contribute to this risk?
- Should COMSEC and COMPUSEC continue to be pursued separately or should they be merged into the pursuit of something broader? Can they?
- Should the government assume the risk of development or should it attempt to persuade industry that a sufficient market exists to justify industry's bearing the risk itself?
- What about information flow? If secure products are the objective, is it better to share technological secrets or to guard them?
- Are the public and private organizations and institutions appropriate to accommodate whatever strategy might be selected? Need they change? What are the impediments to such a change?
- What is the commitment on the part of government and business to information security? How far is each willing to go and how much is each willing to pay or forego?

- To what extent is the provider industry organized and prepared to respond to various strategies? What might be the payoff?
- Whose decision is it anyway? Are the concerns of government, business customers, or industry providers likely to dominate?
- What about the technical challenges? Can the needed devices even be built? Is technology capable of supplying a solution to the information security problem? If so, when, and at what cost?

This paper explores these questions as well as their implications. Written principally from a government perspective, it examines the questions of both difference and separateness.

Part II presents the histories of communications security and computer security in the United States. Chapter 3 briefly traces the evolution of COMSEC during the First and Second World Wars, focusing particularly on the many strategies employed by the U.S. government in those early years to obtain, principally from industry, the various COMSEC devices it needed. Chapter 4 discusses how these disparate strategies gradually gave way to one as the government, through conscious action, was able to secure a monopoly in communications security -- probably to the country's benefit. In Chapter 5, an assault on that monopoly is presented: The president, motivated by a concern over a newly perceived threat to private communications, decides to involve another government department. Chapter 5 discusses the factors that went into that decision and why this "experiment" ultimately failed.

Chapter 6 traces the evolution of computer security, which, in the United States, began with a decade of academic and research interest but without appreciable operational commitment. It discusses the penetrations by "tiger teams" in the early 1970s, which focused attention on the issue within the government's military and intelligence sectors. This motivated several government-funded COMPUSEC R&D tasks and led to the formulation of a single consistent DoD strategy for acquiring desired products from industry. This strategy was given official status with the public announcement of the Computer Security Initiative, which in turn served as the catalyst for the formation of the DoD Computer Security Evaluation Center at the National Security Agency. Chapter 6 also presents the series of computer security activities within the government's civil sector -- a series of laws and regulations that culminated in the passage of the Paperwork Reduction Act of 1980.

In Part III the focus shifts from the past to the present. Chapter 7 describes the current state of information security within both the government and the business sectors. It also discusses the availability of information security products. Chapter 8 examines in detail two opposing views regarding the need for continued separation of COMSEC and COMPUSEC. In addition, it looks at the rationale offered by advocates of two conflicting procurement strategies. Chapter 9 addresses the risks and other stakes involved in the whole question -- economic, political, and security. It examines the nature of the threat to information security and it analyzes the market for information security products. It also discusses how the interests of various players might be affected either by a continued

separation or by a consolidation of COMSEC and COMPUSEC.

Finally, Part IV looks to the future. Chapter 10 expands the menu of possible future courses. Specifically, it explores four alternative procurement strategies involving the various combinations of choices between who bears the risk in producing the products -- government or industry, and in what environment -- classified or unclassified. It explains the four candidate strategies and presents models for each in the form of existing government programs. Chapter 11 looks at various organizations to discover how able they are to react to changes in strategy. And it attempts to answer the question, "Whose decision is it anyway?" Will government, business, or industry concerns ultimately dominate? It then lays out three possible paths that information security might follow.

Chapter 12 takes a final look at information security. It first discusses the power that derives, not from possessing information, but from controlling it. It goes on to distinguish between the use of the word "security" to denote "absence of fear" and its use to refer to the protecting of secrets. Focusing more on ends than on means, it examines just how useful secrecy is in securing freedom from fear.

The report contains no recommendations. It does not even reach a succinct set of conclusions. In the field of information security, if such a field in fact exists, it is easy to find many opinions. Sometimes almost approaching religious convictions, these opinions vary widely. Although some may appear self-serving, most reflect honest differences regarding the direction the country should go in its quest to protect its information. The purpose of this paper is not to decide whose opinion is right, but rather to try to explain why

different people hold different views and what they are. The idea is not to end debate on this important issue, but to focus it.

NOTES for Part I - Introduction

1. Sol Hurwitz, "On the Road to Wired City," Harvard Magazine, September-October 1979, p. 18.
2. Anthony G. Oettinger, "Information Resources: Knowledge and Power in the 21st Century," Science, 4 July 1980, p. 193.
3. Robert J. Herres, "Overview of Computer Security Requirements," text of a speech included as Appendix C in: J. Barton DeWolf and Paul A. Szulewski (ed.), Final Report of the 1979 Summer Study on Air Force Computer Security, the Charles Stark Draper Laboratories, Cambridge, MA, Report Number R-1326, October 1979, pp. 132-133.
4. John Koehler, "The Impact of Computer Security in the Intelligence Community," Proceedings of the Second Seminar on the DoD Computer Security Initiative Program, National Bureau of Standards, Gaithersburg, MD, 15-17 January 1980, p. B-2.
5. M. A. Padlipsky, K. J. Biba, and R. B. Neely, "KSOS-Computer Network Applications," AFIPS Conference Proceedings, 1979 National Computer Conference (Montvale, NJ: AFIPS Press, 1979), p. 373.
6. Carol Bellamy, "The Information Society," a transcript of a sixty-minute documentary produced by Aspen Institute for Humanistic Studies, 1980, p. 18.
7. S. T. Kent, "Network Security: A Top-Down View Shows Problems," Data Communications, June 1978, p. 97.
8. R. Stockton Gaines and Norman L. Shapiro, "Some Security Principles and their Application to Computer Security," Operating Systems Review, Assoc. of Computing Machinery, 12 (July 1978): 19.
9. For one of the earliest expositions on the total security problem confronting computer networks, see Willis H. Ware (ed.), Security Controls for Computer Systems, Report of Defense Science Board Task Force on Computer Security, The Rand Corporation Report R609-1, reissued October 1979, pp. 5-10.
10. Lance J. Hoffman, Modern Methods for Computer Security and Privacy (Englewood Cliffs, NJ: Prentice Hall, Inc., 1977), p. 2.
11. A term sometimes used to embrace both communications and computer security is "network security." For a discussion, see below, p. III-54.

12. The U.S. General Accounting Office has defined information security as "the protection necessary to safeguard personal and other sensitive information processed or stored in a computer system or transmitted and received through a telecommunications network." "It is subject," says the GAO, "to violation at any point from information organization to the final disposition or destruction of the information." (See U.S., General Accounting Office, Federal Information Systems Remain Highly Vulnerable to Fraudulent, Wasteful, Abusive, and Illegal Practices (MASAD-82-18), 21 April 1982, Glossary.)
13. The three words "cryptology," "cryptography," and "cryptanalysis" plus their derivatives are frequently confused. In fact, until 1921, when William F. Friedman coined the term "cryptanalysis," the word "cryptography" was used in the same sense that we would use the word "cryptology" today. Cryptology is the most general term, referring to the science of disguised or secret communications. It embraces the concepts of cryptography, which deals with the science of protecting one's own communications through encipherment or encoding, as well as the concept of cryptanalysis, which deals with solving or "breaking" someone else's ciphers or codes. For a more complete discussion see The New Encyclopedia Britannica, 15th ed. (1980), Macropaedia, vol. 5, s.v. "Cryptology," by Lambros D. Callimahos.
14. U.S., National Communications Security Committee (NCSC), Computer and Telecommunications Security, Report of the Working Group on Computer Security, July 1981, p. 59.
15. Dorothy Elizabeth Robling Denning, Cryptography and Data Security (Reading, MA: Addison-Wesley Publishing Co., 1982), p. 164.
16. For an elaboration on the importance of key management see Rein Turn, "Encryption for Data Security" (Chapter 84-03-01), Data Security Management, Auerbach Information Management Series (Pennsauken, NJ: AUERBACH Publishers Inc., 1982), pp. 11-12. For a more complete technical treatment, see Denning, Cryptography, pp. 164-179.
17. U.S., NCSC, Computer Security, pp. 1-2.
18. D. W. Davies, D. L. A. Barker, W. L. Price, and C. M. Solomonides, Computer Networks and Their Protocols (Chichester, England: John Wiley & Sons, 1979), p. xiii.
19. Greg Lipscomb, Private and Public Defenses Against Soviet Interruption of U.S. Telecommunications: Problems and Policy Points, Program on Information Resources Policy, Harvard University, Cambridge, MA, Publication P-79-3, July 1979, p. 4.
20. "To Our Readers --," Electronic News, 3 January 1983, p. 2.

21. See below, pp. III-2 to III-4.
22. James P. Anderson, Computer Security Technology Planning Study, HQ Electronic Systems Division (AFSC), L.G. Hanscom Field, Bedford, MA, Report ESD-TR-73-51, Vol. 1, October 1972, p. 3. See also DeWolf and Szulewski, Summer Study, p. 71.
23. For a discussion regarding the futility of the "patching holes" approach, see U.S., Air Force, Electronic Systems Division (AFSD), ESD 1974 Computer Security Development Summary, Interim Report MCI-75-1, 31 December 1974, pp. 5-7. See also Roger R. Schell, "Computer Security: The Achilles' Heel of the Electronic Air Force?", Air University Review 30 (January-February 1979): 22-24.
24. Anderson, Planning Study, Vol. 1, p. 4.
25. Ibid., p. 28.
26. J. Michael Nye, Users' Guide: Voice & Data Communication Protection Equipment, National Telecommunications and Information Administration, U.S. Department of Commerce, Report NTIA-CR-80-9, December 1980, p. v.
27. J. P. Anderson, "Accelerating Computer Security Innovations," Proceedings of the 1982 Symposium on Security and Privacy, 26-28 April 1982 (Los Angeles: IEEE Computer Society Press, 1982), p. 91.

PART II

HISTORICAL BACKGROUND

Chapter 3

The Era of Dependence

The point has been made that, in general, communications security devices for use by the U.S. government are developed at the initiative of the government itself. The government pays for the developments and contracts with industry to build them on the government's own terms and according to the government's own specifications. It has not always been so. From the vantage point of the 1920s or 1930s, today's way of doing things would likely have been exceedingly difficult to predict. Then, many COMSEC devices -- even some used in the most sensitive military applications -- were invented outside the government community. Slowly, in an evolution that extended over several decades, the government came to dominate communications security to an extent that today almost seems as unimaginable in computer security as it must have in COMSEC 50 years ago. Whether computer security or the broader information security will follow a like path is hard to predict. A close examination of their respective histories, however, reveals informative parallels and divergences.

The history of modern U.S. devices for communications security began, out of necessity, when the country abruptly found itself engaged in World War I. At the time it entered the war on April 6, 1917, the United States was, according to an official U.S. Army history, "ill prepared both cryptographically and cryptanalytically to meet the great demands which immediately faced it."¹ The country possessed few cipher devices and the sole code in current use, The War Department Telegraphic Code 1915, was known to be insecure and

believed to have been compromised. In fact, according to the same Army history, "it had been reported that a copy was in the hands of the German Government."² Prior to 1917 the official U.S. government policy was one of strict neutrality. As a result, at the outbreak of the war there was no central organization charged with the responsibility of codemaking.³

Fortunately, a private research institute was already engaged in cryptologic studies. The Riverbank Laboratories located in Geneva, Illinois, was directed by Colonel George Fabyan, whose military title had been conferred on him some years before by the Governor of Illinois.⁴ The Laboratories had become involved in cryptologic studies through a staff member's attempts to establish a cryptographic link between Francis Bacon and the works attributed to William Shakespeare.⁵ When a young geneticist on Fabyan's staff displayed an interest in and enormous talent for cryptanalysis, Fabyan placed the man in charge of his cipher department, and offered the services of the Laboratories to the U.S. government. Thus it was that by the autumn of 1916, William F. Friedman, who was destined to become a central figure in all major U.S. cryptologic efforts for several decades, began solving Mexican cryptograms on behalf of Washington.⁶ As Friedman's biographer, Ronald Clark, put it:

The Riverbank laboratories in general, and Friedman's cipher department in particular, thus became the theoretically unofficial, but in practice official, cryptographic service of the U.S. Government.

Before the war, the responsibility for preparing codes for the War Department and the U.S. Army belonged to the Signal Corps. The Adjutant General had the job of "printing, distribution, storage and accounting" of the Army's codes and ciphers. On June 10, 1917,

shortly after the U.S. entered the war, the Army's Military Intelligence Division "established at the War College an organization known as the Cipher Bureau (MI-8)" under newly commissioned First Lieutenant Herbert O. Yardley, who previously had been an employee of the State Department.⁸ Although MI-8, better known as The American Black Chamber,⁹ was established principally as a cryptanalytic organization, an Army document states that it began "to produce its own codes for the use of its military attaches."¹⁰ Thus, between 1917 and August 1921, when the first steps toward consolidation were taken, there were three cryptographic organizations within the U.S. Army.¹¹

The outbreak of World War I created an immediate demand for more secure cryptography. Development of improved codes was accelerated so that "by the time of the Armistice in November 1918, not only had the AEF [American Expeditionary Forces] caught up with their allies but," claimed Friedman, "they had surpassed them in the preparation of sound codes" and "their allies had by then decided to adopt the AEF system of field codes"¹²

Although these improved codes did succeed in enhancing security, they were still quite slow, and more mechanized means were constantly being sought. Toward the end of World War I, the development of such a mechanized device was proceeding, building upon U.S. Army Capt. Parker Hitt's 1915 invention of a strip cipher device.¹³ David Kahn, author of The Codebreakers, writes:

He cut 25 long strips of paper, printed a mixed alphabet on each of them twice, numbered them, and then arranged them in a holder in the order given by a keynumber. To encipher, he slid the slips up or down until they spelled out the first 20 letters of the message in a horizontal line, and then selected any other line, or generatrix, as the ciphertext, repeating this process until the entire message was enciphered.¹⁴

Hitt based his device on one proposed some 24 years earlier by a Frenchman, Etienne Bazeries. Hitt used 25 alphabets in strip form, whereas Bazeries had used 20 alphabets along the perimeters of 20 individual disks comprising a cylinder.¹⁵ Neither Hitt nor Bazeries seems to have been aware that Thomas Jefferson had invented the same basic device during the waning years of the 18th century. Jefferson's device, a cylinder of 36 disks, "was not rediscovered among his papers in the Library of Congress until 1922," according to Kahn.¹⁶

Capt. Hitt brought his device to the attention of the officer in charge of the Signal Corps Engineering and Research Division, Major Joseph O. Mauborgne. In 1917, Mauborgne himself converted the device to cylindrical form and mixed the alphabets much more thoroughly than Hitt had, thereby complicating the task of cryptanalysis. The device became known as the Type M-94 Cipher Device. According to Friedman, the M-94 "was standardized and issued for at least 10 years in the U.S. by the Army, the Navy, the Marine Corps, the Coast Guard, the Intelligence Agencies of the Treasury Department, and perhaps by other agencies."¹⁷

One limitation of the M-94 was that its alphabets remained fixed. Since this impaired the device's inherent security, both the Army and the Navy undertook the task of remedying the restriction. The end result was the Strip Cipher Device, M-138-A.¹⁸ The Army history reports:

It employed changeable paper-strip alphabets, which for the purpose of encipherment were inserted in channels on a metal base. Attempts were made to get the Aluminum Company of America to manufacture these devices but they were unable to do so. In the end, Price Brothers, a small firm in Frederick, Maryland, was induced to attempt to make the devices and succeeded by using laminated bakelite. The first thirty of these devices were manufactured at a cost of

\$15 each and delivered in April 1935¹⁹. . . . The system was placed in operation on 1 July 1935.

Later, the Aluminum Co. of America was successful in producing metal versions. Friedman reports that the M-138-A "was used from 1935 to 1941 or 1942 by the Army, the Navy, the Marine Corps, the Coast Guard, et. al., including the Treasury and State Departments."²⁰

Although certainly faster than codes, these Strip Cipher Devices still did not meet what had by then become a real operational need. By this time, printing telegraph machines had come into use and manual cryptographic systems simply could not keep pace. An electromechanical enciphering device that could operate on-line with the new teleprinters was required. The first such apparatus in the United States was developed in 1918 by the American Telephone and Telegraph Co. as a "simple but ingenious modification" to its printing telegraph machine.²¹ AT&T engineers had begun working on this device in the spring of 1916 and after the war started, were requested by the Signal Corps to continue research into ways of incorporating security into their printing telegraph.²²

The first systems came into use during 1918 and provided service among New York, Washington, D.C., and Newport News, Virginia.²³ The equipment was also installed on circuits that linked Washington with New York and Hoboken, New Jersey.²⁴ An official Bell Labs history records that "a large number were ordered for use by the American expeditionary force in France but were not delivered because of the Armistice."²⁵ In fact, on the day the Armistice was signed, a Signal Corps company organized to install the equipment in France was about to set sail.²⁶

The Printing Telegraph Cipher was the first application of what came to be known as a tape-on-tape (TOT) system. It employed two punched paper tapes, one containing the plain text (the intended message) and the other containing randomly produced key characters. The device electrically combined these two tapes, character by character, yielding the cipher text (the encrypted message), that was finally transmitted. At the other end, the electrical combination of the cipher text with a duplicate key tape restored the original plain text.

Originally the keys were lengths of perforated tape containing characters actually drawn from a hat. As an economy move, these tapes were eventually formed into loops.²⁷ Since the security afforded by the system was substantially reduced every time the loop of keytape completed its cycle and repeated, the engineers designing the system made the keytapes extremely long. However, long keytapes were hard to handle. The scheme was therefore revised by the electrical combination of two short keytapes of unequal (and relatively prime) lengths. Kahn explains:

If one loop were 1000 characters long and the other 999, the one-character difference would produce 999,000 combinations before the sequence would repeat. Thus two tapes each about eight feet long would breed a key that would extend 8,000 feet on a single tape.²⁸

Unfortunately, the two-tape system proved as insecure as it was efficient. The Signal Corps, in October 1919, sent 150 cipher tapes to the Riverbank Laboratories with the challenge to decipher them. The challenge was accepted and on 8 December Colonel Fabyan wired a report of success. An abortive attempt was made at improving the system, but the whole problem was eventually abandoned when the war

ended and there was no longer a perceived need for the machines. Soon thereafter they were discontinued from service and sent to storage.²⁹ So complete was their removal from service that later when the U.S. abruptly found itself once more engaged in a world war and again in need of a printing telegraphic cipher device, not a single one of the AT&T machines was anywhere to be found.³⁰

Kahn wrote of the AT&T device:

Though the device was an engineering success, it proved a commercial failure. Cable companies and business firms, which AT&T hoped would buy cipher attachments for its teletypewriters, passed it over³¹ in favor of the old-fashioned commercial codes.

The codes permitted messages to be substantially shortened, thereby cutting cable tolls, and they provided a modicum of secrecy as well.³²

By far, the most profound development during this period was that of the rotor machine. The rotor machine was later described as the "most important cryptographic device of World War II, and [it] remained dominant at least until the late nineteen fifties."³³ The German ENIGMA, the British TYPEX, and the American SIGABA,³⁴ each one the cryptographic workhorse of its country during World War II, were all rotor machines.

The rotor machine was based on a 1915 invention by Edward H. Hebern. Clark relates that Hebern

designed an enciphering device in which two electric typewriters were joined by twenty-six wires randomly connected, so that a plaintext letter tapped out on one machine would automatically produce an enciphered letter on the second. Six years later, on March 31, 1921, Hebern filed a patent for an enciphering machine incorporating what he called an "electric code".³⁵

Hebern's electric code was what came to be called a "rotor" -- the central component of the rotor machine.

The rotor, or wired wheel, is "a disk about the size of a hockey puck which serves to implement a cipher alphabet." Around the perimeter of each circular face of the disk there are a number of evenly spaced electrical contacts, the number depending upon the alphabet being used. There is one contact for each letter in the alphabet with each contact on the front face wired to exactly one contact on the rear face. Thus, an electrical signal representing a given character will be permuted as it passes through a rotor.³⁶ In a typical machine these rotors are cascaded. In addition, each rotor rotates independently. Thus, a machine consisting of t rotors will not return to its starting position until after 26^t successive encipherments.³⁷

While Hebern was in Washington filing for his patent, he showed his machine to the Navy. The Navy had been looking for an automatic enciphering device for some time and evidenced considerable interest. In 1921 Hebern had incorporated Hebern Electric Code, the first cipher machine company in the U.S. Encouraged by the Navy's interest, as Kahn reports, and "believing -- rightly -- that his new rotor device was the cipher machine of the future, he began selling shares in his firm to raise capital." He thus raised some \$1,000,000.³⁸

By 1924 Hebern had built a five-rotor model that was tested at the Navy Building in Washington. Eventually the Navy ordered two of Hebern's machines, with a promise to buy many more if they proved to be as secure as they appeared to be. To assist in their evaluation of the Hebern device the Navy called in Friedman, who was then in the employ of the Army. After about six weeks, Friedman contrived an attack that ultimately succeeded.³⁹

By itself, this successful breaking of his machines would probably not have killed Hebern's prospects.⁴⁰ But by this time Hebern had become embroiled in legal controversy with his stockholders and was plagued with serious personal financial problems. Also, the machines delivered to the Navy suffered from mechanical problems. The Navy, therefore, decided to discontinue its relationship with Hebern.⁴¹ Clark quotes Friedman as saying that the "Navy dropped negotiations with Hebern when it became obvious that he was not competent to build what the Navy wanted and needed."⁴² Thus, the large Navy contract that Hebern had banked on never materialized and, in spite of a handful of additional sales, his firm ultimately went bankrupt. Hebern died in 1952, without ever being compensated by the U.S. government for his invention.⁴³

With the Navy's decision, the development of a rotor machine became solely a government initiative. According to Clark, in July 1933 Friedman

filed for a patent for what was called simply a cryptographic system. In fact it employed the basic invention of electric control of a set of cryptographic rotors in cascade -- rotors connected in such a way, that is, that each one operated the next one in turn. It was followed in January, 1936, by a patent, the first of its kind, for electrically controlling the vibration of the rotors when they stopped. Then, a few months later, came the patent for a device in which the angular placement of a set of rotors in cascade was in turn controlled by another set of rotors, a device which was to be the heart of the Sigaba, one of America's most used enciphering devices during the Second World War.⁴⁴

The SIGABA, designated M-134, was truly a cooperative venture. The Signal Intelligence Service of the U.S. Army contributed much of the basic design in the form of the Friedman patents. Another part of the Army, the Signal Corps Laboratories in Fort Monmouth, New Jersey,

was given the task of development. The development contract was awarded to the firm of Wallace and Tiernan of Belleville, New Jersey, which the Army history describes as "a relatively small and inadequately-equipped manufacturer."⁴⁵ Despite the equipment's acknowledged value (even before the approaching war made it necessary), the Army could not come up with production funds. It was largely as a result of Friedman's friendship with an Admiral Wenger that the Navy was induced to finance its production. The production contract was eventually awarded to the Teletype Corporation in Chicago, part of the Bell System.⁴⁶

Between 1935 and 1938 the Army became engaged in the development of yet another cipher device, the M-161. It was to be a "small machine for use in combat operations."⁴⁷ Although it was never produced in quantity, its development history (presented in some detail in Historical Background of the Signal Security Agency⁴⁸) offers some insight into the Army's policy governing relations with private industry at that time.

The first mention of the requirement for the M-161 appeared in a memorandum from Major S.B. Aiken to Friedman dated April 24, 1935. The memorandum explicitly set forth "aviation," "mechanized units," and "front line units" as the intended users of the required device.⁴⁹

The original intent, at least on the part of the Signal Intelligence Service (SIS), was to base the M-161's cryptologic design on that of the M-134 (SIGABA), preliminary models of which then existed. The M-161 was given a high priority; it was declared the SIS's most important project. In fact, it was made clear to Friedman that if continued work on the M-134 would in any way delay development

of the M-161, work on the M-134 was to be suspended.⁴⁹

The SIS responded quickly and on October 3, 1935, Friedman announced to his superiors that he was ready to begin discussion with the R&D Laboratories about specific designs and would "hand in draft specs and drawings by October 5."⁵¹

Within the R&D Laboratories, however, the M-161 was not to enjoy the same high priority.⁵² In obvious frustration, Friedman raised the possibility of outside development in a memorandum dated September 10, 1936:

Is it possible that this development could be let by contract to a commercial firm like WE [Western Electric] or GE [General Electric]? In this connection I would like to point out that the Navy has given up trying to develop apparatus of this kind at their labs or shops and are committed to policy of outside development.⁵³

Not surprisingly, this suggestion was not received well at the Laboratories, which replied, "It appears there is little if anything to gain, by farming out this development, even if funds were available. . . ."⁵⁴ The mere fact that the suggestion was made and the fact that the Navy had already embarked upon contractual development, however, are worth noting.

By the following summer the SIS must have learned that the R&D Laboratories were pursuing a cryptologic design different from the one that the SIS had submitted. The SIS therefore suggested that it be given a look at the proposed design lest time and effort be wasted in pursuit of a weak logic.⁵⁵

The reply from the Laboratories admitted that because the original design "was not deemed a mechanical solution," it was not being pursued.⁵⁶ It was becoming clear that the R&D Laboratories' concern was with the device's "military characteristics" whereas the

concern of the SIS was with its security.

Eventually, a preliminary model was fabricated, permitting testing by the SIS. Significantly, for the purpose of their evaluation the SIS "assumed that the enemy had captured one of the machines and therefore knew of its construction."⁵⁷ (Although this is standard practice today, this instance constitutes the first known record of such an assumption by U.S. evaluators.)⁵⁸ In view of the fact that a non-cryptologic organization had designed it, the SIS' verdict was predictable: "The degree of security afforded by this machine is considerably less than that afforded by our present cipher device Type M-94."⁵⁹ Certainly a far cry from that afforded by the SIGABA!

Fortunately, by this time much of the urgency behind the M-161 had passed. This was because even before the security study of the M-161 was made, the Signal Intelligence Service had begun negotiations with Swedish inventor Boris C.W. Hagelin.⁶⁰ Hagelin had begun corresponding with America's cryptologic authorities in 1936, and in 1937 he made a personal visit to the U.S.⁶¹ His invention obviously looked promising because on August 17, 1938, the Signal Corps laboratories were directed to cease all development work on the M-161 "pending results obtained with the Hagelin Cryptographer type E-360."⁶²

When war broke out in Europe in 1939, Hagelin made a second visit to the United States. By now U.S. interest in his machine was even greater. Friedman suggested some improvements to the device and Hagelin returned to Sweden to incorporate them and to streamline the machine for mass production.⁶³

In April 1940 Germany invaded Norway. Hagelin's wife advised that if he ever expected to do business with the U.S., he had better go there right away. Since travel directly to the U.S. from Sweden had become impossible, he went by train to Italy and from there by ship to America, carrying blueprints and two dismantled machines with him.⁶⁴

According to Kahn:

The U.S. Army liked the machine, though it insisted on further tests. Hagelin got 50 machines flown out secretly from Stockholm to Washington for final exhaustive trials. They passed, and after long negotiations, the Army accepted the improved device as its medium-level cryptographic system.⁶⁵

The Hagelin device thus complemented the high-level SIGABA. By 1942 the Smith-Corona Typewriter Company of Groton, New York, was turning out hundreds of the machines; by the end of the war some 140,000 had been produced.⁶⁶ Hagelin's designator for this particular machine was the C-48; the Army called it the M-209.

The Hagelin machines employ keywheels with pins. Dorothy E. Denning, author of Cryptography and Data Security, explains the operation thus:

There are t wheels, and each wheel has p_i pins ($1 < i < t$), where the p_i are relatively prime. The Hagelin C-48, for example, has 6 wheels with 17, 19, 21, 23, 25 and 26 pins, respectively. The pins can be pushed either left or right, and the combined setting of the pins and positions of the wheels determine the key.⁶⁷

Since the p_i 's are relatively prime, the wheels do not return to their starting position until a number of encipherments equal to the product of the p_i 's. In the case of the C-48, this number is greater than 100 million.⁶⁸

As Friedman points out, all of the cryptographic developments

discussed above

fall in the category of apparatus for protecting literal cryptocommunications because the latter employ letters of the alphabet; but apparatus for protecting cifax transmissions, that is, picture or facsimile transmissions, and apparatus for protecting ciphony transmissions, that is telephonic communications, were also developed. But . . . in every case except one, the apparatus was produced by commercial research and development firms with direct guidance from the cryptologists of the Army and the Navy. The one exception is . . . in the case of the extremely high security ciphony system and equipment developed and built by the AT&T Company. It was called SIGSALY.

Within AT&T, SIGSALY was known by a different name. "To the people who worked on it," notes the official Bell history, "it was known as the 'X System,' and it was one of the more closely guarded projects in World War II, and for many years thereafter."⁷⁰

SIGSALY systems, "as finally used during World War II, were not small. A terminal occupied over 30 of the standard 7-foot relay rack mounting bays, required about 30kw of power to operate, and needed complete air conditioning in the large room housing it."

Nevertheless, as the Bell history proudly states, "the system worked."⁷¹

AT&T had first begun working on speech privacy systems around 1920, when it was considering the use of radiotelephone communications.⁷² The following statement appeared in the 1920 AT&T Annual Report:

The problem in attaining privacy in radio telephone transmissions is peculiar and difficult. Nevertheless in the solution of this problem we have also made important progress. Our engineers have carried on conversations by radio telephony according to a method which they devised whereby ordinary receiving stations can hear nothing but unintelligible sounds; yet at all stations equipped with the necessary special apparatus . . . the spoken words can be heard and understood.

The earliest models used speech inversion. Although these models

were found to be unintelligible to the average listener, devices for reinversion were easily constructed and some individuals even learned to interpret the inverted speech. The next step was to split the speech into a number of frequency bands and manipulate each band separately. A workable system, designated the A-3, employed five bands that could be interchanged and transmitted either normally or inverted. Although this afforded better security than the simple inverter, Bell's own history admits that "with the proper equipment the particular combination used by the A-3 could readily be detected and decoding devices could then be built."⁷⁴

During the 1930s Bell engineers experimented with schemes that broke up the speech signal into small time segments and then rearranged the segments. This basic method was discarded, however, because the equipment was too bulky and time rearrangement introduced an inherent delay that users found annoying.⁷⁵

The SIGSALY system incorporated a speech compression device called the vocoder, which had been invented in the 1930s by H.W. Dudley of Bell Laboratories.⁷⁶ By August 1942 a research prototype model was completed. Up to this point Bell Laboratories had carried out the work on its own initiative, although both the National Defense Research Committee⁷⁷ and the Signal Corps were aware of the work and interested in the program.

In February 1941 General Mauborgne,⁷⁸ Chief Signal Officer, made mention in a radio talk of "the problem of maintaining secrecy on the telephone in military service." On April 23, R.K. Potter of Bell Laboratories visited Mauborgne and acquainted him with the prospects for secure speech as Bell saw them. At about the same time that the

experimental system was completed, the Signal Corps decided to sponsor the building of several terminals.⁷⁹

Arrangements were made for Western Electric to manufacture the system at its vacuum tube plant in New York City. By the end of September component part orders were placed. By January 1943 Western Electric was turning out the manufactured items. During the next few months these items were tested and assembled into a complete system, and on April 1 the first system was completed. By the end of April several terminals were installed. The manufacture and installation of the SIGSALY system continued until the middle of 1944.⁸⁰

Late in the war a smaller, much simplified version of the SIGSALY was developed. Called the AN/GSQ-3 by the Signal Corps, it occupied only six 5-foot bays and could be accommodated within a trailer van. Although contracted for in the fall of 1944, none were delivered until March 1946, too late to be used in the war.⁸¹

Another early speech system was the SIGJIP. Whereas the SIGSALY and its successor, the GSQ-3, employed a vocoder to digitize the speech before encipherment, the SIGJIP scrambled the analog signal directly. And whereas the SIGSALY was a large equipment for headquarters use, the SIGJIP was a relatively small tactical equipment. The scrambling method involved dividing the speech signal into 37-1/2 millisecond segments and then rearranging their order according to some key.⁸² The SIGJIP was delivered in 1944 and used on P-51 reconnaissance planes in Europe. According to Howard Barlow, a COMSEC Army officer in Europe who later headed NSA's COMSEC organization, one of the first SIGJIPs flown was shot down by the Germans over Berlin. The Germans, believing it to be the forerunner

of a major new voice scrambler system, immediately launched a sizable cryptanalytic effort against the SIGJIP, which ultimately succeeded.⁸³

As it happened, the Germans' success proved to be of little consequence. For when a new version of the P-51 Mustang came out, the pilots decided that they would prefer to forego the SIGJIP in favor of a tail warning radar in the same location. Thus, the SIGJIP was retired from service after only very brief use. A second factor that contributed to its early demise was a successful analytic attack by two U.S. Army analysts.⁸⁴

By this time a pattern had been established. For every one of the developments just presented, the eventual producer of the devices was a large U.S. company. Initial development models were built either by the firm that had invented the device or by a small company probably operating as a job shop. In The Codebreakers Kahn makes another telling observation:

all the basic cryptographic principles in wide use -- the rotor, the Jefferson cylinder-strip system, the one-time tape, the Hagelin mechanism -- were created by persons with no professional cryptologic background.⁸⁵

Kahn is referring here only to basic principles -- not to actual devices. Clearly, significant improvements to the basic designs were introduced by professional cryptanalysts like Friedman. Nevertheless, the general observation is noteworthy.

Whether Kahn's statement remained true by 1967 when his book was published is perhaps arguable, but it certainly appeared to be true at the time of World War II and for a number of years afterwards. With the gradual buildup of the government's in-house capability and with the advent of electronics, this was destined to change.

Chapter 4

A Government Monopoly

David Kahn wrote of NSA's Communications Security Organization:

It is responsible for the protection of secret American government communications. Consequently it prescribes or approves the systems each department must use and how they must use them. It furnishes some machines itself and lets contracts for the others. It promulgates the national⁸⁶ cryptosecurity doctrine and supervises its execution.

His description is that of a virtual monopoly⁸⁷, but as Chapter 3 has shown, it was not always so. Even as late as the end of World War II, the COMSEC mission was still divided. Both the Army and the Navy operated their own cryptologic organizations, and within the Army cryptographic responsibilities were split still further.

The organizational evolution that would ultimately lead to Kahn's monopoly extended over several decades. The process began a few years after the end of World War I and continued at least until 1952 when the National Security Agency was created.

Throughout World War I, as seen in Chapter 3, military cryptologic activities had been distributed. Within the Army, some functions were assigned to the Signal Corps, some to the Military Intelligence Division, and some to the Adjutant General's Department. The Signal Corps was responsible for code preparation. The Military Intelligence Division was primarily responsible for cryptanalysis. However, an official Army document records that it also "compiled and distributed codes and ciphers for its own use," although apparently it was never authorized to do so. Responsibility for printing, distribution, storage, and accounting belonged to the Adjutant General's Department.⁸⁸

This division had come about as a result of both the national emergency of the war and the natural interests and inclinations of the organizations involved. However, according to the same Army document, it was "soon seen to be a mistake."

For one thing, it led to confusion as to the exact functions of each of the three agencies in the field. For another, the close integration that should exist between cryptographic and cryptanalytic operations was entirely lacking.

The first of these problems was partially remedied in August 1921 when the cryptographic functions of code and cipher compilation were removed from the Military Intelligence Division and consolidated under the Chief Signal Officer, leaving the Cipher Bureau (MI-8) responsible only for cryptanalysis. (This change did not affect the mission of the Adjutant General.)⁹⁰ Chief of the new Code and Cipher Compilation Section within the Signal Corps was William Friedman, who, between stints at Riverbank, had served for a brief time in the Army during the war and now worked for it as a civilian.⁹¹ This arrangement did nothing to integrate cryptographic and cryptanalytic functions and was recognized from the beginning as unsatisfactory. Nevertheless, it was allowed to continue for nearly eight more years.

During this same general period, the Navy integrated its cryptologic functions. This integration was effected by adding a communications intelligence function to what had been exclusively a cryptographic mission. Throughout World War I the Navy's cryptographic effort resided in the Code and Signal Section of the Naval Communications Service.⁹² In July 1922 it was assigned the organizational title, OP-20-G.⁹³ When this unit acquired a pinched copy of the Japanese Naval Codebook in 1921, it could no longer resist

the urge to expand its effort into cryptanalysis as well. Thus, in 1924 a "Research Desk" was added to the Code and Signal Section.⁹⁴

During the next two decades the Navy appeared to place considerably more emphasis on cryptologic functions than did the Army. The Navy spent more money, assigned more people, and bought more equipment. According to Friedman, "for each dollar the Army was able to obtain for cryptanalytic and cryptologic work the Navy was able to obtain three to five dollars" Despite the Navy's quantitative edge, Friedman unabashedly claims that the qualitative advantage belonged to the Army, to whom he attributes "all important developments in both the cryptographic and the cryptanalytic fields" during the years roughly between 1921 and 1939.⁹⁵ If true, whatever qualitative superiority the Army was able to secure must be largely attributable to Friedman himself, for it was to him that the Army would soon entrust all of its substantive cryptologic effort.

In 1929, acting upon the recommendations of Major O.S. Albright, a Signal Corps officer assigned to Army Headquarters,⁹⁶ the Secretary of War integrated under the Signal Corps all of the cryptographic and cryptanalytic activities of both the War Department and the Army.⁹⁷ (The fact that Friedman was in the employ of the Signal Corps was a major factor in this decision.⁹⁸) The Secretary's decision was effected on May 10, 1929, by way of a change to an Army Regulation. The name chosen for the new organization was the Signals Intelligence Service; its director, William Friedman.⁹⁹

This change did not seem to have any immediate effect upon Yardley's "Black Chamber" (MI-8) in New York. What did affect MI-8 was Secretary of State Henry L. Stimson's decision to withdraw State

Department funding on ethical grounds. Although theoretically MI-8 was jointly funded by the War and State Departments, in fact, it was getting most of its support from the State Department. Thus, according to one writer, Stimson's decision "meant instant doom."¹⁰⁰ Interestingly, in spite of the independent decisions of these two Cabinet officers, the Army history reports that "none of the personnel of [the Cipher] Bureau . . . joined the staff of the Chief Signal Officer."¹⁰¹

On August 21, 1934, the next step in the consolidation of cryptologic functions within the Army was taken by the transfer of the printing, storing, distributing, and accounting functions from the Adjutant General to the Signal Corps.¹⁰² Except for name changes, this functional arrangement was to remain intact until after World War II.

During the war there was a need for a rapid buildup of trained personnel. To augment a largely male military workforce, what was now called the Signal Security Agency actively recruited both civilians and WACs -- particularly linguists, statisticians, and engineers.¹⁰³ To help provide training for their technical workforce, the Army turned to the universities.

From the early days of the war, many young engineering officers were assigned to the Signal Corps and sent to successive radar schools operated by Harvard and MIT.¹⁰⁴ The combined curriculum lasted nine months, three months of the basics at Harvard, and the remaining six months at MIT.¹⁰⁵ However, upon graduation, some entire classes from these schools soon found themselves working, not on radars, but on designing cryptographic hardware. There was a real need for

electronic engineers in the COMSEC business and since the most advanced electronics of that time was going into radar, it offered the best available training.¹⁰⁶

Immediately after the war's end another organizational step was taken toward centralized responsibility. As Kahn reports:

On September 15, 1945, a few days after the war ended, the War Department detached the [Signal Security Agency] from the Signal Corps and placed it within the Intelligence Branch (which had tried at least four times during the war to steal it). It was renamed the Army Security Agency and was given authority over all Army cryptologic units, which had previously functioned independently under theater commanders and merely with the advice of the Signal Security Agency.¹⁰⁷

The establishment of the Army Security Agency brought together, for the first time under a single command, all of the Army's signal intelligence and communications security units and people, including field units previously attached to theater commanders.¹⁰⁸ The Army and the Navy efforts, however, remained separate.

The consolidation of the efforts of the two services occurred on May 20, 1949, when then Secretary of Defense Louis A. Johnson created the Armed Forces Security Agency (AFSA) and placed it under the direction and control of the Joint Chiefs of Staff.¹⁰⁹ An investigating committee would later report:

When AFSA was created, the cryptographic activities of both Army and Navy were transferred by the Services to AFSA. At the time, the Air Force had no independent cryptographic unit of its own The State Department and other government agencies had already adopted the practice of relying upon the Military Services for cryptographic service and they have continued to rely upon AFSA. As a result true unification and centralization of this government's cryptographic activities was achieved by the creation of AFSA.¹¹⁰

But the creation of AFSA was intended to unify more than just the U.S. cryptographic effort. It also represented an attempt to consoli-

date the U.S. cryptanalytic effort. Toward this second objective, AFSA was far less successful. At the time AFSA was created both the Navy and the Air Force were opposed to any consolidation. Therefore, by design, the consolidation did not go as far as it might have. Although it did mandate some merging, it left the three services free to maintain their own cryptologic organizations.¹¹¹ There was an attempt, however, to coningle the COMSEC efforts of the Army and the Navy. All of the COMSEC people from the Army's quarters at Arlington Hall were moved to the Naval Security Station in Washington and a merged Army-Navy unit resulted.¹¹²

One of the major problems of this compromise organization was that it had particular difficulty translating intelligence needs into clear targets for COMINT collection. When this weakness manifested itself in the failure of COMINT to warn of the Korean invasion, President Truman, on December 13, 1951, directed Secretary of Defense Robert A. Lovett and Secretary of State Dean G. Acheson to establish a committee to survey America's communications intelligence resources and to recommend any corrective measures it found necessary. The two secretaries quickly appointed a special "panel of distinguished civilians" under the chairmanship of George A. Brownell. A mere six months later, on June 13, 1952, the Brownell Committee submitted its report.¹¹³

Among the findings of the Brownell Committee were that there was still unnecessary and unwanted duplication, that the Director of AFSA lacked any real control, and that there was a high turnover rate among AFSA civilian employees.¹¹⁴ According to one AFSA employee, AFSA "was an agency without a charter or without any clear authority It

had no authority to do anything or to resolve anything."¹¹⁵ The Brownell Committee report itself concluded ". . . that a point has now been reached which makes it essential to carry further the 1949 reorganization," and it called for

. . . a more effective centralization of certain of the COMINT activities brought about by a strengthening of AFSA . . . and an increase¹¹⁶ in its authority over the Service COMINT units. . . .

Significantly, the Brownell Committee found COMSEC to be a non-problem. The report stated:

While cryptography is of itself an advanced, complicated, and important science, it has not been beset by rivalry and strife to nearly the same degree as has the cryptanalytic effort; for this¹¹⁷ reason the cryptographic picture is a relatively serene one.

The report went on to say:

So far as the Committee has been able to determine, our cryptographic activities have been performed without jurisdictional conflict, and without any of the various unfortunate consequences which the Services have often predicted would follow from a unification of other phases of our COMINT capabilities.¹¹⁸

On October 24, 1952, four months after the committee had submitted its report, President Truman signed a presidential memorandum that not only implemented the Brownell Committee recommendations but also gave the revitalized organization a new name -- the National Security Agency¹¹⁹ -- thus concluding more than thirty years of constant organizational transience.

For the COMSEC community at least, the new name was more than symbolic. By 1952 the COMSEC monopoly that Kahn described was all but established. More than mere organizational changes had brought it about, however. Significant changes had also taken place regarding the government's relations with industry. Absent the war-imposed

demand for urgency, the postwar period had offered the government the leisure of instituting a more organized and consistent process for cryptographic development. By building up its own technical base, the government had been able during this period to wean itself of its wartime dependence upon outsiders. This weaning was effected as much out of necessity as of design.

The war had made the government cryptologic community much less naive and far more experienced. No longer were there persons or institutions outside of the government who possessed a comparable degree of cryptanalytic experience and expertise. The cryptanalytic successes of World War II, ULTRA and MAGIC,¹²⁰ had taken care of that. And now that the war was over, the defensive or COMSEC side of the cryptologic community was in a position to benefit from the wartime experience accumulated by the offensive, or cryptanalytic, side.

In late 1945 the Army Security Agency took a significant step that would eventually have a dramatic effect on the move toward centralization. A conscious decision was made within the research and development organization¹²¹ to establish a cryptomathematical research effort applied specifically to communications security. Although partly motivated by "policy frustrations," a much stronger factor in the decision was the simple realization that reliance on outsiders was clearly not working well. Howard Barlow, then in charge of COMSEC R&D, states:

Letting other people do it was a very unsuccessful way of doing business. So . . . people had a policy frustration -- they wanted to be able to do it themselves -- but the driving force was the fact the other system just wasn't very effective

The need was to devise new and original cryptomath principles to meld with the new electronic techniques

rapidly replacing mechanical devices. Also the new COMSEC cryptomath studies were running five to ten years ahead of the current cryptanalytic problems of the Intelligence Community, so only limited input was coming in from the cryptanalytic side.

Lots of people could do engineering for you, but to find someone to develop new principles was impossible -- there just was no background knowledge available. Thus, this searching for new cryptomath principles to go with new electronic¹²² techniques became the essential part of our business.

So, by arguing "that this was an essential part of doing business," Barlow was able to convince Dr. Solomon Kullback,¹²³ then head of ASA's research and development organization, to establish "a special cryptanalytic group . . . to dream up systems" ¹²⁴

The establishment of its own research capability enabled the organization to effect a marriage between mathematical logic design and the different technologies becoming available. As one engineer put it, "Coming up with new ideas were two types of people -- mathematicians and technologists."¹²⁵ A concerted effort was made to fit the cryptomathematics to the particular technologies' specialties. Said Barlow:

The advantage of having your own cryptomath support group was that each of the new digital technologies being explored (transistors, subminiature vacuum tubes, and magnetics) required a different variation of key generator logic to take advantage of the functions each different electronic technique did well, and to avoid¹²⁶ its individual weaknesses. It could be tailor made to fit.

Contributing to the government's emerging independence was an increasing disinterest on the part of industry in the government's business. Although one author has attributed some of this disinterest to "rigorous security clearances" and "oppressive physical security,"¹²⁷ several government engineers who were involved at the time do not believe that security was a deciding factor. Rather,

according to one, it was that many companies were so engaged in commercial product development that they had little interest in government contracts.¹²⁸ The Army still enjoyed good ties with AT&T's Bell Labs, and by this time the Navy had established a close and virtually exclusive contractual relationship with the Teletype Corporation. After the war the Army Security Agency began a search for new sources. A few contracts were awarded to the Underwood Typewriter Co. and to Remington but, according to Barlow, "in general, [these] were not successful."¹²⁹

The first post-war cryptographic devices were off-line rotor machines -- devices which required the generation of the cipher text message as a separate step, as opposed to on-line devices, which are electrically connected directly to the communications equipment and automatically transmit the enciphered message when the plain text message is typed. State-of-the-art cryptographic hardware at the end of World War II involved a combination of mechanical and electronic principles. There were no all-electronic systems at that time.¹³⁰

When the war ended both the Army and the Navy were involved in cryptographic development, and each undertook to develop an off-line rotor machine for its own use. During the postwar period cryptographic machines were given the names of mythological characters and, although distinct equipments, both the Army and the Navy off-line rotor machines bore the same name -- ADONIS. Neither machine included much in the way of electronics. The Army's version, for example, contained but one tube.¹³¹

By now the Army had developed the procedure of first building an in-house model, or breadboard, to demonstrate the principles of

design. It would then seek out capable and willing companies to further the development by taking the device to the advanced development model stage. Usually the development contracts were cost reimbursable and often sole-source -- generally to a company with which the Army was already familiar. The follow-on production contracts, with their added leverage of relatively large quantities of equipment, were normally competitive and fixed price. In the case of the ADONIS, the development contract was a competitive award won by the Anderson-Nichols & Company, Inc. of Boston.¹³² According to Barlow, "they were the least worst" of three or four bidders but, in the end, proved extremely satisfactory.¹³³

The output of the Army version of the ADONIS was a narrow white tape on which characters were printed. The printer embodied a new concept that enabled it to achieve fairly high speeds. The concept had been invented for another purpose¹³⁴ and was later patented by Howard Barlow, Ray Bowman, and Leo Rosen, all of whom then worked for the Army. Anderson-Nichols later incorporated this same idea into one of its commercial printers called the ANILEX, one of the earliest high-speed printers.¹³⁵

Since Anderson-Nichols was not a manufacturing company, the Army was forced to find another company to mass-produce the ADONIS. The government decided upon the Burroughs Corporation of Detroit. In order to reduce Burroughs' initial capital investment and thus induce that company to bid a lower price, the government offered to supply the company with tooling and process drawings. These, the government obtained from Anderson-Nichols. It was through this particular contract that the government's cryptographic community learned an

important lesson -- tooling is not transferrable from one company to another. As one engineer recalled later, "[W]e didn't understand that one company can't design tooling and processing for another company. It doesn't fit."¹³⁶

Now that the Army and the Navy were both separately producing rotor machines for the same basic purpose, both services saw the advantage in being able to utilize the same rotors. Since the Army was further along in its design than the Navy, the Navy changed its design to accommodate the Army's rotors.¹³⁷

Rotors for both versions were purchased under a sole-source contract with Moulded Insulation Company in Philadelphia, at a price of approximately \$200,000. The government not only financed the contract, it also helped the company with the design and special tooling. Later contracts for rotors were competitively won by Honeywell of Minneapolis.¹³⁸

When AFSA was formed in 1949, the Army and the Navy found that they had two similar equipments that were unable to communicate with one another. The developmental models were totally incompatible. This was particularly troublesome for the Marines who had to be able to talk with both services, yet could not afford to be burdened by a need for both machines. A requirement was therefore levied on the Army to develop a version that would intercommunicate with the Navy equipment. Some nine months later, in turn, the Navy set out to develop a version that would intercommunicate with the Army's.¹³⁹

Production economics eventually solved the incompatibility problem. In production quantities, the Army's version proved to be equally reliable and considerably cheaper than that of the Navy

(approximately \$1300 for the Army version as opposed to around \$8000 for the Navy model). The Army version thus became the standard for the U.S. and NATO.¹⁴⁰

After the ADONIS came the ATHENA. Whereas ADONIS had been an off-line machine, the ATHENA was designed to operate on-line. Development of the ATHENA was also contracted to Anderson-Nichols. Later, Frieden won the competitive contract to produce it.¹⁴¹

An ongoing problem with rotor machines helped to spur the development of all-electronic devices. The rotor contacts, aggravated by the harsh elements in which the equipment had to operate, were subject to corrosion that interrupted the electrical current. Eventually, a procedure had to be issued for cleaning the contacts on a daily basis.¹⁴² Yet, despite these problems, rotor machines remain in the U.S. inventory to this day.

There was no shortage of imaginative ideas toward the development of all-electronic devices, and work on such systems was proceeding within both government and industry. As one designer recalls:

We were trying to figure out a way to reduce the ideas to practice. Finally, we started to develop digital circuits -- binary counters and things¹⁴³. . . which now [would be called] logical operations.

Cryptography was about to enter the electronic age.

The earliest electronic cryptographic devices were secure speech equipments. At the end of World War II only a small number of secure voice equipments existed. Those few that did were all narrowband devices, employing either analog scrambling techniques like the SIGJIP or applying vocoder techniques such as the SIGSALY and the AN/GSQ-3. A disadvantage of analog techniques is that they generally can provide only a limited degree of security. And although it is possible to yield good security with

vocoders, the speech they produce is artificial; most speakers end up sounding like Donald Duck. Early vocoders were also large and expensive. Higher rate digital encoding offered a solution to these problems, but at the expense of greater bandwidth and more costly transmission facilities.

As Barlow points out:

It was a tradeoff between . . . narrowband vocoder systems which were bulky, expensive and no one could understand, or you could go to broadband and expensive transmission facilities (except in VHF radio sets where the bandwidth was available), but get high voice quality, and small, cheap equipment.¹⁴⁴

Thus, there was a choice: spend more for the user's terminal equipment or opt for costly transmission equipment.

As was pointed out in the previous chapter, Bell Laboratories of AT&T was involved in the development of at least two secure speech equipments during World War II.¹⁴⁵ The war's end liberated some individuals who had been working on the SIGSALY and allowed them to pursue other digital coding methods. It was during this postwar period that Bell Labs was able to advance the development of Pulse Code Modulation (PCM),¹⁴⁶ which had been invented earlier by Alec H. Reeves of the International Telephone and Telegraph Co.¹⁴⁷ Shortly after the war Army Signals Intelligence at Arlington Hall heard of a new secure voice equipment that was being built at Bell Labs under contract with the Army Signal Corps Labs at Fort Monmouth, New Jersey.¹⁴⁸ The new development was a wideband secure voice equipment employing PCM. With an output data rate of 320 kilobits per second, it could encipher eight channels of voice and was intended for use on microwave links.¹⁴⁹ It was an electronic system and, according to Barlow, technologically ten years ahead of anything else available.¹⁵⁰

The Fort Monmouth people had kept the existence of this equipment from the Arlington Hall staff. When the Arlington Hall people found out about it, they borrowed a copy. Shortly thereafter, Mitford M. Mathews, Jr.,¹⁵¹ then chief of a section in the Ciphony and Cifax Branch, discovered certain security weaknesses in the Bell design. The equipment was modified by the government to correct these weaknesses and then fielded as the AN/TRA-16. Only a few devices were built, however -- enough for but two or three links, all in the U.S. For, in spite of the modification, the AN/TRA-16 was still not judged to be sufficiently secure and was "eventually scrapped."¹⁵² According to Barlow, this case, remarkably reminiscent of the M-161,¹⁵³ "pretty well spelled the end of the Signal Corps going off on their own and developing original cryptosystems."¹⁵⁴

Among the earliest wideband digital voice equipment to be developed by the government's own cryptographic organization was the PEGASUS. It operated at 25 kilobits per second and employed a form of modulation known as Delta Modulation.¹⁵⁵ The equipment was built into a safe with a telephone instrument resting on top and was intended to be used in an office situation. The development contractor was Air Associates of Teeterboro, New Jersey (which later changed its name to ECI and moved to St. Petersburg, Florida). The equipment was fielded during Eisenhower's presidency and one of the engineers recalls that a unit was installed at the President's farm in Gettysburg. Although quite a few were built, the PEGASUS was always viewed as "an interim thing."¹⁵⁶

The replacement for the PEGASUS was the TROILUS. The TROILUS employed PCM rather than Delta Modulation and, because it operated at

double the data rate, it afforded better voice quality. According to Barlow, the particular data rate was carefully chosen. As he explained:

The limiting factor, in those days, was what you could transmit over available transmission lines . . . so, in conjunction with Bell Labs . . . we tried to find out . . . what kind of bandwidth was available.

A convenient and available channel was the bandwidth set aside for AT&T's Carrier System. AT&T had already begun multiplexing voice channels for transmission. The standard method for doing this was Frequency Division Multiplex (FDM) in which twelve voice channels were "stacked" in frequency, 4000 hertz apart, thereby occupying a total bandwidth of 48 kilohertz. By proper line loading, which AT&T was learning how to do, and by dedicating the entire 48 kHz channel to the TROILUS, its 50 kilobit per second signal could be conducted through existing equipment and copper wire distances of 10 to 20 miles.¹⁵⁸

A third secure speech equipment undergoing development at the same time was the NESTOR. Whereas the PEGASUS and the TROILUS were intended for office environments, the NESTOR was designed for field use. In fact, there was an interest from the beginning in being able to locate the NESTOR aboard aircraft. It was therefore a fundamental design objective to build the equipment as small as possible. The NESTOR underwent a lengthy development as it proceeded through a number of versions, each reflecting the progress made in the electronics industry at the same time.

The development of the NESTOR began during the late 1940s. In 1948 the government itself developed the initial breadboard model which employed large vacuum tubes. The fabrication of this breadboard

model made use of hinged aluminum modules, an advanced construction technique later used in several other COMSEC R&D projects.¹⁵⁹

Concurrent with the "in-house" development of the NESTOR, the government contracted with the National Union Tube Company to design and develop a separate speech encryption device. Intended to compete with the NESTOR, it was also to be a small airborne equipment. National Union was in the business of making special purpose tubes and the intention of the contract was to build an entire cryptographic device out of some revolutionary new tubes the company was developing. These new tubes, resembling small television tubes, were designed to scan a digitally coded "target" at the end of the tube. This would enable them to generate a PCM code.

As it happened, the National Union device was never produced. The NESTOR was determined to be the stronger design. However, one of the special tubes was salvaged from the effort and was used in the breadboard version of the NESTOR to perform the analog to digital conversion.¹⁶⁰

After a working breadboard of the NESTOR had been produced, the government awarded a contract to the Philco Corporation to complete NESTOR's development. Philco was provided the logic design by the government and was instructed to design the hardware to that logic design.¹⁶¹

The first Philco model measured approximately 1 foot by 1 foot by 3 feet. Since it had been built with large, tightly packed vacuum tubes, it required a giant fan to keep it cool. Despite this fan, however, the equipment was too hot for reliable operation. It was also too large. Consequently, this vacuum tube version was never

produced in quantity, although a few devices were built for testing purposes and installed in a van and fed into radios for transmission.¹⁶²

The next model used miniature vacuum tubes, but this model was apparently never produced either. By the time it was ready for production, subminiature tubes had become available. According to William P. King, a government engineer assigned to the project, "Every time something new would happen, we'd build a new one."¹⁶³

Subminiature tubes had been developed for applications like hearing aids and, in fact, engineers often referred to this generation of devices as "hearing aid tubes." The tubes were about one inch high and very thin. According to King, some NESTORs using these tubes were built, installed in military aircraft, and flown.¹⁶⁴

Finally, the transistor was announced. (King recalls that soon thereafter the government sent a number of engineers to a Bell Labs-sponsored symposium at Yale University to learn about the new technology.)¹⁶⁵ Philco then built a transistor version of the NESTOR. The original transistors were of the point contact type and proved very unreliable. When these were replaced with the newer "PNP" and "NPN" types,¹⁶⁶ Philco was able to produce a "pretty good" NESTOR, according to King. The final transistor version of the NESTOR was produced not by Philco but by RCA.¹⁶⁷ Later NESTOR models were built with integrated circuits.¹⁶⁸

The NESTOR was to remain in the service inventory for a long time. It saw major use during the Vietnam war and played an important role during the Korea tree-cutting incident of August 1976 by supplying the means for a secure teleconference. Although individual

accounts differ regarding how far down the chain of command the teleconference extended, it certainly included parties in both Washington and Korea.¹⁶⁹

For limited bandwidth channels, the STYX was developed. The STYX made use of vocoder techniques to compress the signal prior to encryption and, like other vocoders, the STYX's voice quality has been described as "disturbing."¹⁷⁰ The STYX represented AT&T's, as well as NSA's, very first all-transistor equipment (it preceded the transistor version of the NESTOR). Therefore, although sharing the problem of voice quality with the earlier SIGSALY and AN/GSQ-3, the STYX was considerably smaller, able to fit into the space of a two-drawer office safe.¹⁷¹ Also, the STYX could accommodate a network of users whereas the SIGSALY and GSQ-3 were restricted to point-to-point use.¹⁷²

King recalls that two multichannel speech equipments were also developed at about this same time. Designated the CERES and the POSEIDON, both were vacuum tube equipments and were developed by the Motorola Corporation in Chicago. According to King, the CERES was a two-channel equipment and the POSEIDON could accommodate up to eight channels. When NSA moved to its present headquarters at Fort Meade, Maryland, the agency used these equipments for its own communications between the new site and its former location at the Naval Security Station in Washington, D.C.¹⁷³

The TANTALUS and the ROMULUS were developed for teletype traffic. The TANTALUS was a multichannel equipment developed for the Navy. It was designed to encrypt two, three, or four multiplexed channels of teletypewriter traffic. The ROMULUS was also a teletypewriter

encryptor but was a single-channel equipment. Both the TANTALUS and the ROMULUS, like the NESTOR, were systems "that took a whole rack full of equipment in the breadboard stage."¹⁷⁴

The development of the TANTALUS began before AFSA was created. It was intended to replace an earlier equipment, the X-500, which never made it into production. The TANTALUS employed magnetic core logic and was a very large device. The development contract was awarded to the Melpar Co.¹⁷⁵

The ROMULUS grew out of what was later described as a "fairly basic research contract" with the Burroughs Corporation to develop key generator logic employing digital magnetic gates. At the time development was begun, the only stated requirement was an internal NSA one. After it was developed, however, it proved quite popular.¹⁷⁶

Like the TANTALUS, the ROMULUS employed magnetic core logic. To drive the magnetic cores required what Barlow termed a "big slug of current" which was supplied by vacuum tubes. Since it was intended as a general purpose equipment, it was designed with a considerable number of options. According to Barlow, "25% of the equipment was taken up with communications options, 98% of which were never used." In spite of the options and the high current, the equipment proved to be highly reliable, with the only significant maintenance problem posed by the vacuum tubes.¹⁷⁷

The ROMULUS was the last cryptographic device to use magnetic cores. The particular nickel-iron alloy used was hard to duplicate, and only Burroughs was successful in establishing design parameters for the cores, which allowed their performance to be predicted.¹⁷⁸

At the time the ROMULUS was being developed, government designers had begun "thinking in terms of some universality in key generators," and it was in this spirit that the PONTUS was developed. The PONTUS was intended to encrypt either multichannel teletype or facsimile transmissions -- in fact, any digital signal within its speed range. Like the ROMULUS, the PONTUS made use of punched cards for its keying material.¹⁷⁹

The PONTUS grew out of an earlier CIFAX device. By this time, however, the demand for CIFAX equipment was very slight. The Air Force used facsimile to transmit weather maps and the Navy used it principally to transmit comic strips to ships at sea. Neither application strongly warranted encryption, and only two or three CIFAX devices were ever built. The PONTUS, as it turned out, fared little better. According to Barlow, only about six of the PONTUS equipments were built.¹⁸⁰ Nevertheless, the PONTUS did serve as the basis for two follow-on versions, one a receive-only and the other a full-duplex device.¹⁸¹

Requirements were now arriving regularly from the military services. Among those involved in COMSEC development during this period was Roland O. Laine. "And once the services started seeing what we could do," says Laine, "their requirements started growing."¹⁸² To meet more requirements, the COMSEC designers found that they already had in hand a basic mathematical approach that could be used. According to Laine:

For the most part, the key generation was probably three to five years ahead of the requirement. I can't remember a requirement that came in that we didn't have ready a technique that could be used straight out or at most modified to meet the requirement.¹⁸³

What the COMSEC designers found they could not anticipate were the particular operational characteristics that might be needed. Although some attempt was always made to satisfy new requirements with existing equipments, this was often not possible. Some unique engineering feature was frequently needed. Such was the case with the JASON.

Around 1952 the Navy came to recognize a personnel problem that quickly translated into the cryptographic requirement that led to the JASON. The Navy had grown to rely heavily on manual Morse code for the bulk of communications with the fleet. Eventually the Navy began to encounter considerable difficulty in attracting and retaining a sufficient number of qualified Morse code operators. In what was later described as a "substantial break with tradition," it decided to replace Morse broadcast transmissions with single-channel radio teletype. Since the Navy wanted the transmissions to be encrypted, it came to AFSA for help. Considering the bitterness that had developed between the two services over the forced merger into AFSA, the fact that the Navy came to AFSA at all could be considered noteworthy. Undoubtedly, the situation that a Naval officer, Capt. Harper, headed AFSA's Research and Development at the time, helped to break down some of the barriers.¹⁸⁴

The Navy's requirement presented the AFSA engineers with a thorny technical problem. The transmission was intended to be a continuous one-way broadcast with the receiver maintaining radio silence. This made cryptographic synchronization difficult for the receiving station. What was needed was some way for a receiving station to synchronize itself with the transmitting station even if it had failed to receive the beginning of the transmission, and also to regain

synchronization if, for whatever reason, the receiving station lost it. To meet this need the AFSA COMSEC engineers applied the concept of "clock synchronization" and included in the new equipment a catch-up mode that allowed the receiving station's key generator to run at a speed different from that of the transmitting station.¹⁸⁵ JASON was built by the Burroughs Corporation.

JASON employed the hearing aid type of vacuum tube, and while developing JASON the government discovered a trait of these tubes that yielded a significant improvement in tube life. Conventional wisdom held that coated filaments were to be preferred over uncoated ones because they offered better electronic emission. Higher filament voltage was also known to improve electronic emission. What the government learned, however, was that by using tubes whose filaments were uncoated and operating them at only 25% of their rated filament voltage, sufficient emission could be obtained for their use in digital circuits and the improvement in tube life was extraordinary. The performance thus achieved by the JASON was impressive. In spite of its 600 vacuum tubes, the equipment dissipated but 75 watts of power and, according to Barlow, achieved a tube life of 20,000 hours, sufficient to permit the epoxy mounting of the tubes on printed circuit boards.¹⁸⁶

Thus, by the end of the 1950s NSA and its predecessor organizations, responding to diverse requirements, had successfully designed and fielded cryptographic equipments for a wide variety of uses and environments. Still, there was a significant environment left -- space.

At the time NSA first became involved in building cryptographic machines for use in satellites, it knew little or nothing of what is involved in developing or producing space qualified equipment. NSA did, however, have a rather clear idea regarding the logic design that would be needed.¹⁸⁷

The Air Force wanted cryptographic devices that would be compatible with its planned Space Ground Link Subsystem (SGLS), which was intended to combine in a single, compact flight package all of the separate modules required for the command and control of various spacecraft. The intention was to multiplex telemetry, tracking, and command data over a single radio frequency link instead of transmitting these various signals over different links as had been the practice.¹⁸⁸

The requirement was to build two cryptographic systems, one for the ground-to-satellite link (uplink) and the other for the satellite-to-ground link (downlink). King reports that it was NSA's desire "to build something that would be producible and would be an item for the Air Force general inventory. . . ." Since TRW was the Air Force's prime contractor for the SGLS, and because compatibility was deemed so important, NSA contracted with TRW to build a Command Security System (CSS) and a Low-Speed Telemetry Security System (TSS). The CSS was to protect the uplink signals, whereas the TSS was to protect the downlink. This, according to King, occurred in the early 1960s.¹⁸⁹

Ironically, the cryptographic devices fared better in the marketplace than did other equipments in the parent systems. In King's words, "Each space program wanted to build . . . their own equipments, anyway, so the actual TRW hardware for the SGLS didn't get

used by everybody, but . . . the key generators did"190

NSA's success in capturing this last new market of space was important and not without difficulty. Air Force program managers, responsible for large, expensive satellite programs, typically depend on the economic club offered by incentive contracts for their management control over their contractors. The last thing a program manager wants is for the contractor to fail to meet the terms of the contract, yet get paid as if he had. This can occur if the contractor is able to blame his lack of performance on the government. Thus, from the program manager's point of view, the more independent of the government the contract can be made, the better. Any equipment that the government is obliged to provide is a potential escape clause for the contractor and is instinctively avoided by space program management organizations. In this environment it was far from inevitable that the NSA would succeed in establishing itself as the sole supplier of cryptographic hardware for U.S. satellites. Yet that is what happened. The CSS and the TSS were but the first of a family of NSA developments of space equipments.

Thus, the government's cryptographic effort, focused at the NSA, had shown itself capable of producing a wide variety of cryptographic equipments designed to protect everything from tactical voice communications to satellite telemetry. Any help it was now obtaining from industry was on the government's own terms. Inside the U.S., the major market for cryptographic products lay within military and intelligence circles. That market was limited, well understood, and controlled. Foreign markets existed, but these were quite effectively controlled by license requirements and export restrictions.¹⁹¹ For

all intents and purposes, then, the only cryptographic development that took place was that which the NSA desired to take place. The government, through the NSA, had indeed acquired a virtual monopoly. This monopoly, which can be roughly dated to the agency's creation in 1952, went largely unchallenged for almost a quarter of a century.

Chapter 5

A Challenge to the Monopoly

Until the early 1970s the cryptographic monopoly remained largely intact, and official U.S. cryptography remained the forbidden province of the Department of Defense. Not that there were not others engaged in cryptography. A number of amateur cryptographers and cryptanalysts have always been active, but cryptography for most of them was a hobby -- something they did for diversion. And there were several commercial firms that produced cryptographic devices but their major markets lay outside the U.S.

Then, in the mid-1960s a National Data Center¹⁹² was proposed. Sensitized by the press and aroused by politicians, public opinion gradually caused personal privacy to become a hot political issue.¹⁹³ Although much of the concern was directed at the government itself, the dramatic growth in the number and scale of private data links gave rise to additional worry. A report by the Congressional Research Service stated, "The proliferation of large government and private recordkeeping systems compounded by the extensive use of automated data processing" came to be "viewed as a threat." During the 93d Congress alone, "upwards of 200 bills pertaining to privacy were introduced."¹⁹⁴

Out of these concerns grew a demand for protection. Fears about both foreign and domestic invasions of privacy led many private firms and individuals to demand security for their stored computerized files and for their electronically transmitted messages.¹⁹⁵

By itself, the increase in demand probably would not have led to very significant action. However, at the same time politics created the demand, technology provided an opportunity. Until now, cryptography had been very expensive and was regarded as a dreaded nuisance. The advent of integrated circuit technology changed this and brought high grade cryptography within the practical reach of a much broader market.¹⁹⁶

The response to this new set of conditions was swift and occurred initially on two fronts -- within the research community and within government. Later, industry would be swept up in the tide as well.

Mathematicians, computer scientists, and engineers in business and academe began displaying an interest in cryptology. As Kahn wrote, "Very rapidly the quantity and quality of information on cryptology being circulated outside of government channels exceeded by far what it had ever been before."¹⁹⁷

According to Whitfield Diffie, writing in January 1981:

the two most conspicuous results of this expanded interest [in cryptology] have been the promulgation of a cryptographic standard by the National Bureau of Standards and the development of public key cryptography by university researchers.¹⁹⁸

At least to the extent that these two developments were the result of the expanded academic interest, they were its cause as well.

Interestingly, NBS' involvement in cryptography grew out of its program in computer security. In a quest for an efficient and economical method of encryption that might be compatible with a variety of computer systems, NBS solicited "information and suggestions" for an algorithm that was eventually to serve as a Data Encryption Standard (DES).¹⁹⁹ The initial solicitation was published

in the Federal Register in May 1973. According to a Senate report, "That solicitation evoked few responses and a second solicitation was issued in August 1974." NBS asked the NSA for help in evaluating the proposals and "in consultation with NSA," selected the algorithm submitted by IBM.²⁰⁰

The algorithm submitted by IBM as a DES candidate was derived from one that it had already developed for itself and its own customers. The IBM algorithm, called LUCIFER, came in response to requirements, particularly from overseas banks and Lloyds of London, to protect computer-to-computer communications.²⁰¹ Although similar in fundamental design to the original LUCIFER, the DES employed a greatly reduced key size -- 56 bits as compared with LUCIFER's 128.²⁰²

The entire DES review process, from 1973 through 1977, promoted an intense discussion of cryptography within a now-awakened academic community. Almost immediately, various members of the research community let it be known through the scientific press that they had reservations about the security of the DES.²⁰³ Some even suspected, as an article in Science magazine pointed out, that the DES had been "carefully designed to be just secure enough so that corporate spies outside the government could not break a user's code and just vulnerable enough so that the National Security Agency (NSA) could break it."²⁰⁴ NBS attempted to mute the outcry by hosting a pair of workshops that dealt specifically with the strength of the algorithm. The workshops, however, did not succeed in stilling all the criticism, and in 1978 the Senate Select Committee on Intelligence formally investigated NSA's involvement in the development of the DES. The

committee concluded that although NSA had been instrumental in getting IBM to restrict the key size, NSA had not tampered with the design of the algorithm in any way.²⁰⁵

Not everyone outside the government deprecated the DES. In fact, many saw it as a significant advance. M. Blake Greenlee of Citibank observed that, "Compared to other encryption devices used by banks, DES is a great step forward."²⁰⁶ Even Robert Morris of Bell Laboratories, who had been a proponent of a larger key size and had argued for the revelation of additional design principles, wrote, "[I]t is plainly superior to any commercially available encryption device I have seen. I believe it will serve any ordinary commercial purpose for a good many years to come."²⁰⁷

The concept of public key cryptography was advanced in a singularly important paper by Whitfield Diffie and Martin Hellman of Stanford University, published in 1976.²⁰⁸ Whereas traditional encryption schemes use the same key to govern the enciphering process as well as the deciphering process, the Diffie-Hellman proposal was to use two different keys, one for enciphering and the other for deciphering.

As one writer pointed out, a major disadvantage of traditional schemes including the DES is that they "require the advance establishment of a private key between every pair of correspondents and thus [do] nothing to alleviate the increasingly complex problem of key management."²⁰⁹ The basic idea behind the Diffie-Hellman proposal was that by making use of "one-way functions" (i.e., functions whose inverse is extremely difficult to compute), the function itself or enciphering key could be made public while the inverse function or

deciphering key could still be kept secret. Public availability of the enciphering key would allow anyone to create a secret message, but only someone in possession of the deciphering key could decipher the message.²¹⁰

The Diffie-Hellman paper only postulated the existence of an appropriate mathematical function possessing the desired one-way property; it did not offer such a function. Of course, absent a specific implementing proposal, the basic idea was not very useful, albeit quite clever. However, in the next few years concrete implementing schemes began to be advanced.²¹¹

Thus, these two developments, the DES and public-key cryptography, served to open the flood gates of academic research. Since technical research feeds on itself, the result has been an increasing proliferation of articles, researchers and results. In Diffie's words, this has

had the effect of legitimizing the field as a specialty in computer science, electrical engineering, and to some extent, mathematics This interest is abetted by the connection of cryptography with a number of other fields of current interest in mathematics and computer science.²¹²

And Kahn writes:

Today a net of mathematicians and computer scientists trade high-powered ideas on new cryptosystems and how they can best be used. Where once two or three cipher machine patents were issued in a year, now half a dozen are issued every month For the first time in history, there is a broad, economically-motivated interest in cryptography outside the government.²¹³

As Diffie points out, cryptography has proven "valuable to researchers both as a source of new problems and as a field of application for existing results" ²¹⁴

While all this was taking place within the academic community, the government was very active as well. Specifically, it responded with new laws, new policy, and a new government player.

The new laws dealt with the issue of personal privacy. Four such laws were passed between 1970 and 1974 and later summarized in a Congressional Research Service report. The first was the Fair Credit Reporting Act (Public Law 91-508), "which gives an individual access to his consumer credit records and allows for procedures to correct erroneous data." One provision of the Crime Control Act of 1973 (P.L. 93-83) "limits the use of criminal records and permits correction of erroneous data." P.L. 93-380, the Education Amendments of 1974, addresses the issues of privacy and accuracy of educational records. Finally, the Privacy Act of 1974 (P.L. 93-579) "gives an individual access to records concerning himself, and the right to copy, correct and challenge personal information held by the Federal government." It also requires that a list of all federal government files containing personally identifiable data be published in the Federal Register.²¹⁵

The new policy, which took the form of a presidential directive, derived not so much from a concern for privacy as from a concern regarding foreign eavesdropping. On November 16, 1977, National Security Advisor Zbigniew Brzezinski, in the name of President Carter, signed Presidential Directive/NSC-24, commonly referred to as PD-24, which called for "improved telecommunications protections for government-derived, unclassified information which may be of value to a foreign adversary."²¹⁶

Although promulgated relatively early in the Carter presidency, the new directive did not represent some sudden initiative of a new administration. The issue had been brewing for some time. The directive reportedly grew out "of more than four years of secret deliberations"²¹⁷ on the part of national security advisors of both Carter and former President Ford²¹⁸ "about ways to secure public and private telephone messages, transmitted throughout the United States by microwave towers or satellites, against interception efforts by the Soviet Union and perhaps other countries."²¹⁹

In the fall of 1976 the Director of the Office of Telecommunications Policy (OTP) during the Ford administration was asked by the National Security Council (NSC) to draft "a coherent system plan" that would address regulatory, legal, and economic issues attendant to communications protection. Among the more difficult questions the U.S. government faced was how it could protect networks that it did not own. An OTP staffer recalls that the plan was delivered to the National Security Council during the first week of December 1976. By that time the election had taken place and action on the plan was deferred until after Carter's inauguration.²²⁰

On the twenty-second of January the Director, OTP, received a call from a member of the Carter NSC who advised, "We've received this technology applications study and its legal, regulatory, and economic issues, and something needs to be done with it. Would you please come over and talk to us?" It was decided during a series of discussions between the OTP and NSC that the Director, OTP, should chair an interagency study group to make recommendations on how to deal with the overall subject. The events of this study group ultimately resulted in what would become Presidential Directive-24.²²¹

In at least two important ways the directive was revolutionary. It officially acknowledged for the first time that even some unclassified information required protection; and, also for the first time at least since the days of Yardley's Black Chamber, it assigned responsibility for the protection of some U.S. government communications to an agency outside of the DoD. The directive set down the policy that all government unclassified information "useful to an adversary" should be protected and nongovernment information useful to an adversary "shall be identified and the private sector informed of the problem and encouraged to take appropriate measures."²²² In some very carefully worded distinctions, the directive redistributed protectionary responsibility as described below.

Presidential Directive-24 defined communications security (COMSEC) as being "concerned with protective measures designed for the security of classified information and other information related to national security." It assigned responsibility for COMSEC, thus defined, to the Secretary of Defense. Nothing new there. The directive then introduced the term "Communications Protection" involving "government-derived unclassified information (excluding that relating to national security)." This responsibility, along with "dealing with the commercial and private sector to enhance their communications protection and privacy," the directive assigned to the Secretary of Commerce.²²³

The question of where to assign responsibility was indeed a thorny one. Because the perceived need for protection extended beyond the national security community to the civil sector, there was

"considerable reluctance to let the Department of Defense be solely in charge."²²⁴ A New York Times article quoted an administration official as saying, "We didn't think it appropriate to have the Department of Defense controlling the civilian sector."²²⁵ DoD's agent for COMSEC then as now was the NSA and what was really being said, according to NSA's former director Admiral Bobby R. Inman, was "that you have to have two elements because you couldn't trust an intelligence organization to be involved in the part of communications security which related to the private sector."²²⁶ Inman recalls attending a meeting as a vice director of the Defense Intelligence Agency at which this issue was being discussed. He reports, "That was my first exposure to the strong political views held by [some NSC staffers] . . . that never, under any circumstances, would it be appropriate for an intelligence agency to have access to the communications of American citizens for whatever reason." According to Inman, it was not that anyone believed that the NSA was actually "looking at domestic communications or was even likely to," but rather, the NSC staffers simply wished "to draw organizational lines that would preclude that ever occurring."²²⁷ During the mid-1970s, in the wake of Watergate, even the appearance of government spying or intrusion had become a "high politics" issue.

The preferred solution would have been to give the job to some organization above the cabinet level, but the most obvious was the Office of Telecommunications Policy (OTP), which was about to fall victim to Carter's plan to reduce the size of the White House staff. According to Donald E. Kraft, who was assigned to the OTP at the time:

If the Office of Telecommunications Policy had stayed in existence, there's no doubt in my mind that the

responsibility would have been placed there . . . and the Director of Telecommunications Policy would have been responsible for orchestrating the effort . . . but . . . [when] OTP was abolished, . . . there wasn't a place²²⁸ above the Secretarial level to place this responsibility.

Thus, the job of monitoring the DoD and DoC activities under the program was assigned to a special committee headed by Frank Press, Carter's science advisor.²²⁹

In spite of this vestige of centralized control, the real effect of the policy was to divide responsibility for protecting government communications between the DoD and the DoC. Moreover, the division was to be according to the type of information -- very close to the concept of content. The division was made neither according to who possessed the information nor according to who owned the communications link. Either of these might have been harder to defend rationally but would have been immensely easier to administrate. The problem, of course, was that any given link serving any given agency might carry a wide variation in content at different times. The directive did not address this problem.

Nor did the directive specify measures. A strong but unstated assumption underlying the new policy was that classified equipments, as NSA-produced cryptographic devices tended to be, were not suitable to protect the unclassified, non-national security information within the DoC charter. In most cases, the environment in which the equipments would have to operate could not accommodate classified devices. Moreover, the equipments, procured in limited numbers and built to military specifications, were expensive. And for most envisioned applications, the NSA devices amounted to overkill. They were more robust than the threat seemed to demand.

Thus, the directive left the DoC with two difficult jobs. It had to contrive a way to carve out its own piece of the action and it had to devise a new strategy for protecting government communications that would be independent of the NSA and its products.

To carry out the tasks assigned to the DoC by the new directive, the Secretary of Commerce selected the National Telecommunications and Information Administration (NTIA).²³⁰ NTIA was a brand new player,²³¹ having very recently been created out of the old Office of Telecommunications from within the DoC and the Office of Telecommunications Policy, which had been part of the Executive Office of the President.²³² To carry out its communications protection function, the NTIA established a Special Project Office.²³³

In retrospect, the selection of the NTIA might appear strange since the NBS, also part of the DoC, was already deeply involved with cryptography. But at the time the issue was being debated, it was not perceived as a cryptography issue at all.²³⁴ Rather, it was seen as a policy issue. The question of how the government might go about protecting networks it did not own was seen more as a legal question than as a technical one. Cryptography was considered as but one of many possible solutions. Even more decisive was the fact that most of the OTP people involved in the planning were being transferred to the NTIA. There was no one elsewhere within the DoC who had been at all involved in the issue up to that point. According to Kraft, "When many of the functions and staff members were reassigned to the Commerce Department, the communications protection function just came with them."²³⁵

The newly formed Special Projects Office within NTIA wasted no time in setting an ambitious agenda for itself. In a presentation to the National Electronics Conference in 1979, Kraft and another NTIA official, Charles K. Wilk, outlined some of their agency's current and projected activities relating to communications protection. These included:

- "determining just what types of . . . government information are sensitive or 'useful to a foreign adversary.'"
- "collecting information on protection techniques."
- characterizing the strengths and weaknesses of the public communications network.
- "determining how the evolving carriers' networks 'might' be made less vulnerable."
- "exploring the basic national strategies and options for implementing telecommunications protections."
- studying the effect of alternative policies on the private sector.²³⁶

Kraft and Wilk further stated that "NTIA's primary concern is in the development of a national strategy and implementation plan to assure that adequate protections are available . . . "; that NTIA's activities would "strive to encourage the development of commercial protections and innovative technologies, with minimum disruptions to industry structure . . . "; and that "maintaining a competitive environment [would] remain an important objective."²³⁷ To perform these functions, the Special Projects Office was organized into three branches: a Policy Branch and a Survey and Training Branch in

Washington, and an Engineering Branch located in NTIA's technical laboratory in Boulder, Colorado.²³⁸

Despite its lofty plans, NTIA's Special Project Office for communications protection never really got off the ground. Some studies were sponsored and a course was developed,²³⁹ but the Special Project Office was unable to gain the requisite bureaucratic foothold that could have ensured its survival.

The NTIA had two options. It could join forces with NSA and jointly develop and pursue a strategy for protecting unclassified, non-national security communications. Or it could attempt to carve out, either by charter or by precedent, its own piece of the action and pursue that piece as independently of NSA as possible. It appears that NTIA tried both and neither worked.

Among the specific tasks that flowed from the issuance of PD-24 was one assigned to the Secretaries of Defense and Commerce jointly. The president's science advisor asked them to draft a "joint plan." Kraft saw it as "the typical program manager's road map" -- something science advisor Press could use "in overseeing the direction and measuring the progress of the implementation of the directive." Kraft relates:

We got together with the people at NSA and began to work on such a plan and they immediately said, "Oh you surely don't . . . really want us to have a plan for protecting classified information. We already have that plan. That's the National COMSEC Plan. That's our plan to do our half of the job. We'll look over your shoulder, Commerce, and help you prepare your plan." And, they made it stick, and right there was a problem. Instead of having one plan to show how these two agencies were going to work together to achieve a solution, each agency had a special plan. Now you've got two different agencies separately pursuing a solution to the same problem. If they don't come up with the same answer, one solution is suspect. If they reach the same conclusion, much work has been duplicated.²⁴⁰

Meanwhile, the NTIA leadership apparently decided to define NTIA's niche and to seek authority through legal mandate. Thus, they devoted much of their managerial time, effort, and attention to the development of a clear and generally acceptable definition of their role and mission. This became a significantly greater task than they had anticipated. Specifically, NTIA attempted to find a sensible way to distinguish between information related to national security and that which was not. That effort, according to one NTIA official, was a complete failure.²⁴¹

That the effort ended in failure should have been no surprise, given the nature of the problem. Myriad difficulties confront the division of responsibility for information protection according to content. The distinction between unclassified information that is of national security interest and that which is not is murky and elusive enough. For example, is it possible for one of the military services to possess any information at all that is not national security oriented? Even if this and similar questions could be answered satisfactorily and the necessary distinction made, many, many very difficult questions remain. For example:

- How does one deal with the problem of aggregation, i.e., individual items of information that by themselves have no national security significance, but that in combination, do?
- Since links can contain both classes of information, should an attempt be made to protect these classes separately? If so, how?
- If only 5% of an agency's data should fall into the national-security related category, to whom should the agency

go for help? Specifically, must it deal with both the DoC and the DoD?

-- Should a link be protected according to the most sensitive data ever to be passed over it or should some other standard be applied? If so, what should be the standard?

It is important to observe that if all of these question were to be answered conservatively -- that is, by opting, when in doubt, for the highest form of protection -- the DoC would be left with precious little to protect.

Early on, NTIA's top management realized that trying to divide responsibility according to content was not going to succeed. Henry Geller, then Assistant Secretary of Commerce for Communications and Information and NTIA's Administrator, actually refers to the job his organization was given as "Mission Impossible." As Geller says, "[T]here was no feasible way to identify content that should be protected; rather, channels that at times carry such information should be protected." He notes, however, that there already existed a classified process for protecting channels. In order to make his task more realistic, Geller proposed a revision to NTIA's charter to officials of the Executive Office of the President but was turned down. This negative signal understandably influenced the priority that the Special Project Office was to enjoy within the NTIA.²⁴² NTIA compounded its difficulty by allowing itself to be trapped in a definitional paradox with respect to threat. Since its principal source of authority came from PD-24²⁴³ and PD-24 mentions only the protection of non-national security information from foreign threats, NTIA seems to have confined its full attention to this area. It was

discouraged, both from within the DoC and by the Office of Science and Technology Policy, from offering protection against threats that originated from within the United States. As an NTIA staff member stated:

Basically, the threat to our telecommunications, as posed by PD-24, lay with one potential adversary and some very specific geographic locations and, if the threat were not that particular adversary, that was not PD-24 work.²⁴⁴

Not surprisingly, it was hard to argue that information in which there was sufficient foreign interest to need protection had no national security significance. Wilk relates an anecdote that tells the story quite well:

I remember being asked to go over to the FBI and talk with a couple of people They're worried about their agents going to make a bust . . . and they find that either the crooks are gone or forewarned or the newspaper people are there, because they're using the telephones . . . , and I had to ask them, "Is there a threat of any kind from this particular foreign adversary . . . ?" When they said, "No," I had to say . . . , "I'm sorry, but we can't be involved in that."²⁴⁵

Apparently, the NTIA did not view privacy protection of personal data as an appropriate object of their attention either. This despite several facts that seemed to argue otherwise: it had already become the object of increasing concern within the federal government; outside of the DoD's own information, the Defense Department was essentially ignoring it;²⁴⁶ and PD-24 specifically mentions it. The directive advocates efforts "to adopt system capabilities that protect the privacy of individual communications. . . ."²⁴⁷ The General Accounting Office noted NTIA's hangup with foreign threats when it reported in 1980:

. . . since NTIA has not considered electronic transmission containing personal data useful to adversaries, it has no

ongoing effort to develop guidelines for protecting personal data in the telecommunications environment.²⁴⁸

Another problem was internal. As Geller himself admits, the Special Projects Office did not enjoy a high priority within NTIA. From Geller's point of view, it made little sense "to pour top management efforts" into what he had already decided was "a seriously flawed [mission] assignment."²⁴⁹ This lack of management support was clearly felt at the working level. In Wilk's words:

We did not have a whole lot of close management attention at NTIA. I mean, this was a weird project It didn't fit. People's attention was always somewhere else We were kind of tolerated, at best.²⁵⁰

Thus, whenever the Special Projects Office went forward with a proposal to expand its operation, it was repelled by the NTIA management. Even when the the Special Projects Office presented its case directly to the president's science advisor, it was unsuccessful.²⁵¹

Besides suffering from disinterest from within, NTIA was plagued to some extent by unrealistic expectations from without. The civil agencies, perhaps quite naturally, saw NTIA as their NSA. Said Massey:

What NSA did in the classified arena, in toto, they [the civil agencies] expected us to be able to do for this whole field of sensitive, non-national security, and of course, . . . we never began to have the "horses" to do it.²⁵²

Which brings us to one last problem. Even if the Special Project Office had succeeded in fashioning a clear and acceptable mission statement and received strong management support from within, it probably would not have been sufficient to have guaranteed NTIA's survival. A clear mission statement would have specified for whom and against whom NTIA was supposed to be working, but would not have

spelled out exactly what NTIA was supposed to be doing about it. This would have required a degree of technical competence that NTIA seemed to sorely lack. As one senior Department of Commerce official bluntly put it, "I think the people who got the job were incompetent in the security field and had no way of getting competent."²⁵³ A DoD official who had been closely involved throughout the "NTIA experiment" adds:

They had no skilled people; their mission was unclear and undefined and they had poor leadership They had no credibility with the people²⁵⁴ that counted -- the government agencies and the carriers.

Not only did NTIA lack competence, but it also seemed incapable of acquiring it. Inman attributes this shortcoming to the fact that NSA had the market cornered. "Competence wasn't available that could be hired on the street NSA did have a monopoly of talent" declares Inman.²⁵⁵ However, such an explanation is probably overly simplistic. Other organizations, even within the government, when faced with the urgent necessity of acquiring a technically sophisticated workforce, have found ways to do so. Geller admits as much. Although Geller acknowledges NTIA's lack of competence, he believes he could have overcome the problem had he chosen to do so. He points to discussions with "intelligence community officials" who offered him help in this regard. However, since he had already concluded that he had been given an impossible assignment, he did not pursue the issue.²⁵⁶

The original idea was that any technical work would be assigned to the Engineering Branch in Boulder. According to Wilk, the Boulder group had heretofore been principally engaged in frequency propagation studies, and included people with backgrounds in science, mathematics,

engineering, and computers. One even had "some background in cryptography." Wilk recalls:

What they were going to do was to learn what sort of crypto equipment is available in the private sector; to become -- I'll say expert -- but certainly not in the way NSA is expert. And I have to say that my reading of the situation was that they were not able to do as much as they hoped.²⁵⁷

According to Wilk, some of what they attempted to do was met with resistance from NSA.²⁵⁸ The Boulder effort also apparently suffered from some of the same management indifference that afflicted other parts of the Special Projects Office, and distance likely proved a barrier as well. For whatever reasons, delegating the technical work to the Boulder group did not work well.

Despite all of these problems, Inman still believes that the split could have worked. However, NTIA lost the one individual who could have given it the best chance of succeeding, and in its attempt at independence, NTIA apparently overdid its drive to distance itself from the NSA. When NTIA was first established, Paul I. Bortz, an applied mathematician from Denver, was selected as its number two man. Bortz was a problem solver. He enjoyed NSA's respect and was an individual with whom the DoD agency could have worked. But Bortz's tenure was quite short. When he left, instead of proceeding to solve problems, according to Inman, NTIA set out to build a bureaucracy by "constantly demeaning NSA and raising all kinds of speculation."

Inman reports:

Much of the speculation that came out in the press that we [NSA] were deliberately trying to undercut the security of communications available in the private sector, etc., came out of NTIA.²⁵⁹

This had the effect of souring Inman on the organization. Having

concluded "that it would never be a productive, effective organization," he decided that the Special Project Office had probably outlived its usefulness. As Inman himself puts it:

. . . it was the work out on the sidewalks to try to keep raising the spectre of NSA as the threat to the privacy of American citizens by people inside NTIA, clearly done for bureaucratic growth purposes, that eventually led me to an absolutely hardened view about them.²⁶⁰

Inman went on the attack. He made a deliberate and conscious decision to abandon what he called NSA's traditional "policy of absolute public reticence."²⁶¹ In the fall of 1978 he granted an interview with Science magazine's Deborah Shapley and in January 1979 he spoke before a symposium of the Armed Forces Communications Electronics Association.²⁶² His decision was partially motivated by what he perceived as an unwillingness on the part of NTIA to "recognize the legitimate role of NSA" in the overall COMSEC problem.²⁶³ Says Inman:

They [NTIA] were not prepared to say there were national security concerns . . . and that, in no small degree, contributed to my eventually going public on the topic and trying to build a constituency separately and to impact on the decision-making apparatus of Congress²⁶⁴

Inman sought out the media because he perceived that it was the media who were primarily responsible for shaping the views of both Congress and senior Executive Branch officials. He reports that, once he went on the attack and the media gave what he called a "balanced accounting," he found the attitudes in Congress and in the Executive Branch "less apprehensive" toward NSA.²⁶⁵

The specific remedy Inman had in mind is clear from this statement he made in 1981:

I do not find the results of four years' separate effort very productive, and if I were making the decision, this

would be one area in which I would do some early swift surgery to cut the size²⁶⁶ of the government bureaucracy and go back to a single body.

Inman's "hopes" for NTIA were advanced with the arrival of the Reagan administration. The new administration was looking for non-defense related activities to cut; NTIA had been established under Carter and had been controversial from the beginning. Almost immediately, NTIA began to feel a squeeze on its budget. When the assault began, there were few to be found willing to rush to NTIA's defense. In fact, were it not for Congressional support from such people as Senators Barry Goldwater (R-Ariz.) and Larry Pressler (R-S.Dak.), the overall cuts on the NTIA might have been much deeper.²⁶⁷ As one author put it, NTIA's budget authorization went "from indefinite to year-to-year, perhaps matching the mood of fiscal austerity ruling Capitol Hill but possibly a harbinger of future difficulties."²⁶⁸

As far as the Special Projects Office itself was concerned, however, the cuts for FY83 were quite deep enough. On October 1, 1982, the Special Projects Office of NTIA was essentially cut to one person. One year later it was scheduled to disappear entirely from the organizational chart, formally ending the NTIA experiment and bringing to a close a unique chapter in the history of COMSEC.

Although not necessarily planned as such, the NTIA experiment was a challenge to NSA's COMSEC monopoly. But the experiment had failed; the challenge had not succeeded. Whereas high politics concerns had been responsible for NTIA's creation, it was mostly difficulties at the level of low politics that ultimately led to its demise. Some even say the creation of NTIA was fatally flawed from the beginning -- that it could not have worked. Dr. Harold J. Podell of the General

Accounting Office, for example, states:

You can't have two authorities on the same subject in the same government. You can only have one It's a fundamental technical issue. You either have one person who is the ultimate authority or you have none, on any technical issue in any organization, and I think the NTIA experience was trying to violate that fundamental principle of technology I feel the fact²⁶⁹ that events took care of themselves tends to verify [this].

In spite of the failure of the experiment and the demise of the organization, there are those who believe that some good had been accomplished. As Massey puts it:

Well, look at it this way. When you look at our broad charter, we were supposed to do something about raising awareness; we were supposed to do something about encouraging the private sector; and I think all of this has been done. You can look out at the commercial world, and there are quite a few vendors who are putting out pretty good protection equipment. There is a higher level awareness for the need for this kind of thing. So I can't, in my own mind, say that we were a²⁷⁰ total bust -- far from it. . . . Things were happening!

Not all view the NTIA experiment as a positive step. Raymond T. Tate, who headed NSA's COMSEC organization at the time, believes that, rather than constituting a move in the right direction, the experiment "delayed the needed cure by years."²⁷¹

As the NTIA faded out of the communications protection picture, the NBS might have appeared to be a possible candidate to assume its role. According to an earlier study, even former NTIA officials have admitted that NBS possessed superior technical expertise.²⁷² However, it is far from clear that NBS ever wanted the job. If assigned to the NBS, the task would almost certainly have been delegated to the Institute for Computer Sciences and Technology (ICST), which has had the DES responsibility. But ICST's Director, James H. Burrows, has even expressed some apprehension over the fact that his group has the

DES. Specifically, he has strong reservations about advancing the state of public knowledge of cryptography when that knowledge might be used to strengthen the COMSEC of other countries and thus deprive the United States of useful intelligence it is now able to obtain. Further, he has stated that he was never sympathetic to the view that the responsibility for communications security could or should have been split in the first place.²⁷³

Thus, whether by default or design, even before the signing of NSDD-145, the National Security Agency found itself rapidly becoming the de facto, if not the de jure, manager of all government COMSEC -- both national security and non-national security. The official replacement of PD-24 to reflect this fact has long appeared inevitable.

Chapter 6

From Task Forces to Kernels to Laws

Compared with communications security, computer security within the government has a much briefer history. 1967 appears to be the year when computer security began to receive some official attention within both the Central Intelligence Agency (CIA) and the Department of Defense (DoD). The CIA in 1967 recognized computer security "as a unique security discipline" when that agency appointed a "Special Assistant for Automatic Data Processing within the Office of the Director of Security."²⁷⁴ Within the DoD, also in 1967, the Advanced Research Projects Agency (ARPA) initiated funding for the development of the ADEPT-50, the first recorded general purpose operating system designed to implement DoD security policy. The ADEPT-50 was developed by the Systems Development Corporation to run on the IBM/360.²⁷⁵ Finally, on the policy side, 1967 was the year that computer security was raised as a pressing issue within the DoD.²⁷⁶

At that time resource-sharing systems were being procured in increasing numbers for government installations and the problems of security for them were becoming of "pressing concern" both to the military and to their contractors. In April 1967 direction was sought from the Office of the Director of Defense Research and Engineering, and in June 1967 the Director of the Advanced Research Projects Agency (ARPA) was asked to form a task force. A series of discussions among government, industry, and academic people were held during the summer and fall of that year. Finally, in October the task force began

meeting under the chairmanship of Willis H. Ware of the Rand Corporation.²⁷⁷

The Ware Task Force, in addition to DoD, industry, and academic members, also included representation from the CIA. Thus, from the very beginning the COMPUSEC efforts of the DoD and the CIA were at least loosely coupled. The task force was directed "to study and recommend appropriate computer security safeguards that would protect classified information in multi-access, resource-sharing computer systems."²⁷⁸

The task force succeeded in describing the computer security problem in greater technical detail than had previously been done, it set forth both technical and policy recommendations, and it outlined some areas that needed further work.

One of the more immediate results of the Ware Committee report was the creation of another DoD task force. In February 1970, according to a report prepared for a U.S. Senate committee, the Department of Defense ADP Security Task Force was formed

to develop necessary security policy directives utilizing the advanced technology in automatic data processing systems. The products of this task force were Department of Defense Directive 5200-28, "Security Requirements for Automatic Data Processing (ADP) Systems," and its companion "DOD ADP Security Manual 5200.28M" of January 1973.²⁷⁹

Among its provisions, the directive called for the establishment of a central DoD capability for:

- a. Assisting and advising DoD Components in ADP System security testing and evaluation;
- b. Assessing progress of DoD Components toward development and effective installation of secure ADP Systems.²⁸⁰

This provision generated considerable discussion regarding the appropriate degree of authority of the organization chosen to serve as this "central DoD capability." Some saw it as some kind of czar that would decree which computers could be procured and which ones could not. Others, obviously chagrined at even the hint of such an abrogation of autonomy, saw the organization as nothing more than a repository of information -- a library. During the controversy at least three separate DoD organizations came forward and offered to take on the job -- the Navy, the NSA, and the office of the Deputy Under Secretary of Defense for Policy. All offers met strong resistance. As one official was later to observe, "It struck me that . . . it doesn't make any difference who sticks their neck up out of this crowd, they're going to get shot."²⁸¹ Eventually, the idea of a "central capability" was abandoned.

About the same time the policy documents were being written, teams of penetrators, known as "tiger teams," were formed to determine the vulnerability of computer systems to penetration. According to one account, their

record of success in penetrating all commercial systems attempted led to the perception that the integrity of computer systems hardware and software could not be relied upon to protect information from disclosure to other users of the same computer system.²⁸²

By the early 1970s the teams had compiled extensive lists of the various ways systems could be penetrated.

In one of the more notable cases, a tiger team broke into the Honeywell MULTICS system²⁸³ on the very day that the system was first put on public display. The team was attempting to decide if MULTICS was capable of handling sensitive military functions.²⁸⁴ According to

one author, "Prior to the 1970's, no commercially available system had withstood penetration, and no existing system could adequately enforce multilevel security."²⁸⁵ A 1974 summary report by the Air Force's Electronic Systems Division (ESD), which summarized the results of several of these penetration studies, stated:

Most penetration efforts have been completed successfully with very few (perhaps two) man-months of effort. Typically the bulk of the effort expended is directed toward exploitation Development of the basic approaches . . . has usually required only a man-week or two. In comparison, the effort expended in patching operating system holes is rumored to be in the tens or hundreds of man-months.²⁸⁶

According to another writer:

Even those systems that underwent "retrofitting" to correct known implementation errors and design oversights²⁸⁷ were penetrated with only moderate amounts of energy.

During the early 1970s the Air Force Electronic Systems Division sponsored several studies aimed at developing techniques to support the design and verification of multilevel security systems.²⁸⁸ The first of these studies came as a direct result of a security analysis of the computers used by the Air Force Data Services Center (AFDSC). The AFDSC wanted to operate its computers in an "open multilevel" environment. The result of the security study was that "no set of modifications" to a computer's operating system "would render it suitable for multilevel operation, much less for open operation with uncleared users and terminals."²⁸⁹

Following this discouraging finding, according to the ESD summary report:

. . . the Air Staff directed ESD to convene a computer security technology planning study panel. The panel, composed of recognized experts from industry, universities, and government organizations, convened in early 1972. The panel operated under a contract from ESD to James P.

Anderson and Company, and was tasked with preparing a development plan for a coherent approach to attacking the problems of multilevel computer security.²⁹⁰

Among other things, the Anderson panel recognized the futility of "patching" known faults in existing operating systems²⁹¹ and recommended to start "with a statement of an ideal system, a model, and to refine and move the statement through various levels of design into the mechanisms that implement the model system."²⁹²

The basic component of the panel's ideal system was called a "reference monitor," which the ESD summary defines as "an abstract mechanism that controls access of subjects (active system elements) to objects (units of information) within the computer system."²⁹³

The reference monitor itself is nothing more than an abstract concept. The mechanism that implements it in hardware and software is called the "security kernel." Although the basic notion of security kernel does not imply any particular balance between hardware and software, the security kernel in many systems often embraces software alone because the hardware is predetermined.²⁹⁴ Regardless of the hardware-software balance, three characteristics are required of a security kernel:

1. It must be tamper proof.
2. It must always be invoked.
3. It must be verifiably complete.²⁹⁵

Stated another way, the security kernel must be large enough to satisfy all of the security requirements of the system, yet small enough to permit the establishment of its correctness.

Since the amount of work involved in software verification is greatly magnified as the number of lines of code is increased, kernels

were always thought of as relatively small things. As one article put it:

Because of the need to prove that the security relevant aspects of the kernel perform correctly,²⁹⁶ great care is taken to keep the kernel as small as possible.

At the time security kernels were first conceived, only very short programs consisting of a few hundred lines of code had been successfully verified. Thus, it was far from clear that the simultaneous achievement of the three goals was even realizable in a practical sense. The situation is only a little improved as of 1985.

Neither the fundamental notion of a security kernel nor its name originated with the Anderson Panel. The basic idea grew out of some earlier work at ESD involving Roger R. Schell, then an Air Force Major. Schell conceived the notion of what he later described as a "subset of the hardware and software that was sufficient to provide security even if the remainder of the system" had been produced "by an adversary." In search of a name for this bold new concept, Schell went to Dr. John B. Goodenough, then an applied mathematician at ESD. By Schell's own account, he asked Goodenough, "What would you call this?" Goodenough replied, "Well, that seems to be a lot like the notion of kernel in mathematics and since it relates to security, why don't you call it a security kernel?" Since neither Schell nor fellow researchers at the MITRE Corporation had any other ideas and since Schell was due to submit an abstract for an upcoming conference, he accepted the Goodenough proposal. Later, the ESD-MITRE group learned that the Digital Equipment Corporation had independently chosen the name "kernel" to refer to the most privileged state in their PDP-11 but this, according to Schell, was pure coincidence.²⁹⁷

Toward the ultimate objective of building a security kernel, several R&D efforts were initiated between 1972 and 1976. In 1972 the MITRE Corporation began an effort known as the Brassboard Kernel Project, which attempted to build a kernel-based operating system from scratch. In 1973 SRI International initiated a design study called the Provably Secure Operating System Study (PSOS). An important result of these early studies was the emergence of a process for system design specification that would prove very useful in later developments. Between 1974 and 1976 MIT, Honeywell, and MITRE were each engaged in designs of a security kernel base for MULTICS. At UCLA work began in 1974 on a security kernel base for a specialized piece of systems software for the DEC PDP-11 computer. In 1975 Honeywell was awarded an Air Force contract "to design an improved hardware base for use as a Secure Communications Processor (SCOMP)." Finally, in 1976 additional research efforts were started at MITRE, UCLA, and the Systems Development Corporation (SDC). The MITRE and UCLA efforts were aimed at developing "trusted prototypes of the UNIX (TM) operating system," whereas the SDC effort was an attempt to develop a "kernelized version of the IBM VM370 operating system (KVM)."²⁹⁸

Sponsorship for these projects was diverse. Some projects were funded by the NSA, DCA, and ARPA, but by far the most significant funding came from the Air Force. In 1976 this abruptly changed. Schell writes:

In August 1976 Air Force System Command directed termination of the Electronic Systems Division's ADP System Security Program. Termination was completed by September 1977, halting development (that was proceeding well) of a secure general purpose prototype to fully demonstrate operational acceptability and the associated development of

specifications, policy recommendations, and evaluation
criteria for general use.²⁹⁹

A combination of factors appears to have contributed to this sudden decision. In the first place, problems arose within the Air Force itself when various echelons that had previously supported the ESD work began to lose interest. Secondly, there was a problem within the Pentagon. The particular staff organization whose support was almost essential began to question the direction the program was taking.³⁰⁰ Schell recalls that this difficulty within the Pentagon was attributed to undercutting by individuals from both government and industry. According to Schell, these people voiced opinions that questioned both the objective and the approach of the Air Force program.³⁰¹ Apparently, the voicing of such opinions was at least sufficient to plant doubts. Finally, and perhaps most decisively, a funding problem arose in Congress. According to Schell, the problem with Congress never would have occurred had the program retained Air Force backing.³⁰² However, it did not retain this needed support and the program was cancelled upon actual direction from Congress.³⁰³

This cancellation of funding caused considerable scurrying for alternate sources of support. By this time ARPA had assumed the overall direction of the computer security program for the DoD. In 1974 ARPA hired Stephen T. Walker from NSA to manage the program. Although Walker had no prior COMPUSEC experience, he possessed an extensive background in computer engineering and, according to Walker, the ARPA leadership must have believed that anyone from NSA surely knew something about computer security.³⁰⁴

In January 1975 Walker established the ARPA Technical Working Group. Previously, individual researchers in computer security

working under ARPA sponsorship had corresponded regularly and kept each other informed of the current status of their research, but there had been no attempt to organize the interchange or to schedule it on a regular basis.

In 1976, when the Air Force announced its funding decision, it fell upon Walker to locate alternate sources of both money and technical direction. Supplying the needed technical direction proved the more difficult task. To lead a particularly critical project, Walker decided that the best candidate in the DoD was a young NSA professional, Daniel J. Edwards.³⁰⁵ Having served as a member of both the 1969 Ware Task Force and the 1972 Anderson Study Committee, Edwards possessed a considerable background in computer security. There were two problems with Edwards, however. Edwards worked at NSA, and NSA had a contracting procedure that was known to be slow and burdensome. An attempt to award a contract through the NSA process would cause a hiatus that Walker wished to avoid. Walker's solution was to use ARPA money and ARPA's more streamlined contracting procedures. The second problem, according to Walker, was that Edwards' NSA boss felt reluctant to give up a talent as great as Edwards' for what was now a non-NSA task. When Walker then offered the job to the National Bureau of Standards, NSA had second thoughts and responded favorably to Walker's proposal. Thus, in August of 1977 a contract was awarded using ARPA's contracting procedures and funding from ARPA, NSA, and DCA, but with Edwards named as the official technical representative of the government (Contracting Officer's Technical Representative, or COTR, in the DoD's parlance).³⁰⁶ Through a series of such strategies, Walker was able to

mitigate somewhat the effect of the Air Force's pullout although the largest and most significant project, MULTICS, had to be dropped.³⁰⁷

Several of these early efforts were aimed at developing prototype systems. According to James J. Cooke, Vice President of the MITRE Corporation, it was during one such effort

that the computer security community came to realize fully that the experience and discipline for building and supporting general-purpose computers was a very limited national resource and lay almost exclusively with those companies who did that for a living -- the commercial computer vendors -- and further, in their computer operations!³⁰⁸

When Walker transferred to the Office of the Secretary of Defense in late 1977, the DoD focus for computer security transferred with him. In March 1978 the ARPA Technical Working Group gave way to the Computer Security Technical Consortium. This did not constitute a direct replacement. The Consortium, composed entirely of DoD people, functioned primarily as a means of disseminating information, whereas the Working Group had been a real technical forum used to test new ideas.³⁰⁹ In June 1978 the Computer Security Initiative was officially launched. The announced purpose of the Initiative was "to achieve the widespread availability of 'trusted' ADP systems for use within the DOD." The Computer Security Initiative represented the DoD's selection of an acquisition strategy. It constituted a conscious attempt "to foster the development of trusted ADP Systems through technology transfer efforts and to define reasonable ADP system evaluation procedures to be applied to both government and commercially developed trusted ADP systems."³¹⁰ Under the aegis of the Initiative, a series of seminars was held at the National Bureau of Standards in Gaithersburg, Maryland.

There was still the matter of who was to be in charge. Hoping to obtain some direction, Walker briefed his bosses, Dr. Gerald P. Dinneen, Assistant Secretary of Defense for Communications, Command, Control and Intelligence [ASD (C³I)], and Dinneen's principal deputy, Dr. Robert J. Hermann. Having spent many years at NSA himself, Hermann's immediate reaction was, "That's an NSA problem. Give it to them. Let [their COMSEC Organization] do it."³¹¹ Hermann apparently believed that the computer security problem fit naturally with the communications security problem. After arguing unsuccessfully that COMPUSEC was a fundamentally different problem, Walker returned to his office to try to reconcile the guidance he had just received with what he believed he might be able to sell to the services, who had unanimously opposed locating the COMPUSEC responsibility at NSA only a few years earlier.³¹²

On the one hand, Walker realized that if the central DoD computer security activity were located anywhere other than NSA, the question, "What does NSA think?" would always arise. On the other hand, Walker was keenly aware of the strong feeling among the services that they would be much better off if they did not "let NSA into their knickers."³¹³ The services foresaw much interference and little immediate help. NSA had the reputation of working endlessly to produce the technically perfect product and, in the meantime, providing nothing but criticism of whatever solution the services might conceive on their own.³¹⁴

After pondering various options, Walker concluded that NSA was the best place for the activity, but somehow the effort had to be independent. He became convinced that the problem could not be

assigned to an existing organization -- particularly the COMSEC Organization. Walker conceived the idea of a Program Management Office similar to an existing arrangement for the management of the Washington-area Community On Line Intelligence Network (COINS) also located at NSA. When he put forth this proposal in the fall of 1979, the idea was rejected as being too complicated. Walker was told that the DoD could not tolerate another "administrative anomaly" like COINS and he was directed to think of another solution.³¹⁵ By this time Dr. Harry L. Van Trees had replaced Hermann, and Walker assumed that Van Trees was responsible for the rejection.³¹⁶

Hoping to get some fresh ideas, Walker met with his immediate superior, Dr. Thomas P. Quinn, during January 1980. Out of this meeting came a totally new proposal. Recognizing that the government computer security problem extended beyond the DoD, the two thought of proposing a government-wide computer security center. Since the National Bureau of Standards (NBS) already had an official responsibility for rendering technical advice on computers to the rest of the federal government, they decided that NBS might constitute a logical (and acceptable) location for such a center. The idea was that the DoD would supply, initially at least, the bulk of the technical expertise and financial support; NBS would offer a government-wide charter and perspective as well as a politically benign home.³¹⁷

In pursuit of this idea, Walker met with James H. Burrows, Director of the Institute for Computer Science and Technology at NBS.

When Burrows supported the idea, Walker decided to brief two top officials within the NSA. In March 1980 Walker met with Howard E.

Rosenblum and Kermith H. Speierman, Deputy Directors for Communications Security, and Telecommunications and Computer Services respectively. Walker briefed them and gave them a copy of his proposal (Appendix A). He left with the distinct feeling that he had failed to convince them.³¹⁸

This feeling was reinforced the following month. In April 1980 Vice Admiral Bobby R. Inman, then Director of the NSA, met privately with Dinneen, who was still the ASD(C³I). Although not present, Walker gathered from questions Dinneen later asked him that Inman had some strong reservations. At this point Walker decided that he needed to talk to Inman. Their meeting was originally scheduled for 4 June, but the celebrated computer failure at the North American Aerospace Defense Command Headquarters in Colorado forced a delay.³¹⁹

The meeting finally took place on 4 August. Walker began the meeting with an historical recounting, throughout which he recalls that Inman simply sat passively and listened. However, as soon as Walker got to his proposal for a Federal Computer Security Evaluation Center at NBS, Inman erupted. "'I've had nothing but trouble from those Commerce guys,'" Walker quotes Inman as saying. As the conversation continued, it became clear to Walker that Inman's principal problem had been with another part of Commerce, the National Telecommunications and Information Administration (NTIA),³²⁰ but it appeared to Walker that Inman was willing to tar any part of the DoC with the same brush.³²¹

According to Walker, Inman went on to say that he would never allow the DoD to become a partner with the DoC in any venture as

important as computer security, and threatened to go to the president if necessary to prevent such an occurrence.³²²

By his own admission, Walker had certainly not anticipated such a strong reaction. But before he could regain his composure or make a graceful exit, Inman adopted a more conciliatory tone. First, referring to Walker's earlier proposal for a program management office at NSA, Inman told Walker that he had heard of the proposal and had wondered what had become of it. Inman agreed that there was a real need for such an organization and said that he thought that doing the job within the Defense Department made "a great deal of sense." He went on to say that he would be willing to set up a Program Management Office at NSA as Walker had originally proposed.³²³

At this point, Walker, apparently wishing to avoid any misunderstanding, said, "[L]et's make sure we understand that this should not be done in the same way that COMSEC is done." Inman agreed and told Walker he understood. Walker then quotes Inman as saying "I don't want this to come back to my organization yet. I've got a little work to do here. But, if you give me a letter that asks me how I would do this as a Program Management Office, I will respond to you with what it would take" According to Walker, his letter went out on 3 September and Inman's reply was dated 7 October.³²⁴

Inman did not need much time to reply because he was already at work on the idea. Unbeknown to Walker, the agreement hammered out with Inman at their stormy meeting was identical to one Inman had worked out with Dinneen months before.³²⁵ Although Walker knew that Inman had met with Dinneen, he apparently was unaware that there had

been two such meetings nor had he been told of the substance of the meetings.

When Inman first heard about the NBS proposal, it must have conjured up visions -- all bad -- of his earlier, and still lingering, relationships with NTIA. Inman states:

It was that [the NTIA] experience that propelled me into action when I saw the proposal being floated in Defense that would have had us join together for a computer security program that again dealt with the whole government.³²⁶

Inman did not wish the NSA to become involved in computer security for the entire government. He believed

that the needs in much of the government were substantially separate from those of defense and . . . could see us getting into arguments over . . . standards³²⁷

Inman felt that if the problem were limited to Defense, there might be hope of coping. It was in this light that Inman sought his meetings with Dinneen.³²⁸

In addition to concluding that NSA's COMPUSEC involvement should be limited to the DoD, Inman decided that whatever new computer security responsibility NSA might be given needed to be established as a separate organization.

Inman believed that the different nature of the security requirement argued against placing it within the COMSEC organization. In his view, the level of protection required in most computer security applications is substantially lower than what the COMSEC organization was accustomed to, and in his perception, would be intent on providing. Says Inman:

I don't believe that the same standards apply at all for the bulk of computer security where the information is much more perishable.³²⁹

Inman saw the security need in COMPUSEC more nearly matching that of tactical systems whereas he saw COMSEC as applying more to strategic systems. He was particularly afraid that higher-than-necessary computer security standards would ultimately lead to "systems that were vastly more complex and vastly more expensive than . . . needed and, in turn, that would limit the use."³³⁰

Inman was also concerned about internal priorities, fearing that if he should place COMPUSEC in an already existing organization, it would tend always to be viewed as a stepchild and "not . . . [as a] principal point of concern."³³¹

At the same time, Inman concedes that he wished "to draw on the engineering talent and the thoughtfulness in the communications security area."³³² Ultimately, Inman decided to set up the COMPUSEC unit as a separate entity but to staff it with a number of people from the COMSEC organization as well as from other parts of NSA.

Although successful in forging an agreement in principle, Walker still faced another problem -- time. Dinneen was already letting it be known that he probably would resign at the end of the president's current term, regardless of the outcome of the upcoming election,³³³ and Inman would reach the end of his nominal four-year tour as NSA Director the following summer. At this point, both Dinneen and Inman understood the issues involved and were ready to take action. Quick action from a new set of players on a matter of such complexity and controversy seemed highly improbable. Thus, if Walker failed to submit a proposal to the Secretary of Defense level before January, he would likely be back to "square one."

Walker still faced the non-routine task of obtaining concurrence, or at least comment, from each of the services and defense agencies. He was fully aware that the agreement he had forged with Inman would not receive unanimous approval.

Around the third week of October Walker revisited the NSA. By this time Inman had delegated the job of interacting with Walker to Walter G. Deeley, Deputy Director for Programs and Resources. Deeley recalls his instructions from Inman to move quickly. "I want to do it before Dineen goes out of office," Deeley quotes Inman as telling him.³³⁴ During their meeting Deeley urged Walker to waste no time in getting the matter to the SECDEF level since Deeley believed that Secretary of Defense Brown also probably intended to resign regardless of the outcome of the now-imminent election.³³⁵

On the day before the election, Walker met with Deeley a second time. At this meeting both decided that they were ready to go to the services for comment. Walker sent a memo on 11 November and asked that comments be returned by 12 December. By Walker's own admission, that was "an incredibly short time for something like this."³³⁶

According to Walker, the comments ranged from "This is a good idea. Let's do it." to "My God, what a terrible thing. It's really bad!" Walker recalls puzzling for some time over the best way to present the results to his bosses. By this time, of course, the election was over. The Democrats had lost, so most of the people above Walker's level were preoccupied with finding new jobs.³³⁷

Fortunately, the comments did contain one common thread of agreement -- that something like a Computer Security Evaluation Center

was needed.³³⁸ Disagreement centered on exactly what it would do and where it was to be located.

To present the disparate results, Walker created a two-dimensional matrix with the respondents along one axis and the major points of contention along the other.³³⁹ He also drafted a memorandum for signature that acknowledged "some concern about working relationships within the proposed Evaluation Center" but pointed out that there was "no disagreement or doubt regarding the need" and approved "the proposal made by the Director, National Security Agency to establish a Program Management Office."³⁴⁰

Walker recalls carrying the package to Dinneen's office on 23 December while the office was in the midst of a Christmas party.³⁴¹ Time was definitely running out. Walker had no reason to expect action on his memo before the end of the holiday season and by then less than three weeks would remain before President-Elect Reagan's inauguration.

However, on the 26th or 27th, Dinneen approved the memo and sent it forward. On 3 January, Walker saw the memo again. Deputy Secretary of Defense W. Graham Claytor, Jr. had signed it the day before. (See Appendix B.) Walker was flabbergasted. He had been certain that this was one of those matters that a lame duck incumbent "would leave for the next guy." Walker paid another visit to Deeley at NSA. Walker describes Deeley as "ecstatic." "'Congratulations!'" he quotes Deeley as saying, "'That was the smoothest bit of stuff I've ever seen.'"³⁴²

Walker's euphoria was not destined to last long. On 24 January it was announced that Inman was leaving NSA to become the Deputy

Director of Central Intelligence.³⁴³ What worried Walker was that, with Inman gone, it would take the civilian leadership of NSA little time "to straighten out this 'mistake' Inman had made."³⁴⁴

On his next visit to NSA, Walker was introduced to the man Inman had appointed to serve as the first director of the new center, George Cotter. Walker recalls his frustration: "I kept going out to NSA and meeting new key people." Nevertheless, he began what became a long series of productive meetings with Cotter and, in April, they began to draft a DoD directive intended to serve as the charter for the new center. The charter required not only the agreement of Walker and Cotter, but also concurrence from the military services. Obtaining this proved to be difficult. Walker describes drafting and coordinating the directive as "one of the more interesting frustrations I've had in a long time."³⁴⁵

The major objection to the original draft charter came from the Air Force, whose principal concern was what degree of control the center might be given over service budgets for computer security R&D. A personal meeting between Gen. Robert T. Marsh, Commander of the Air Force Systems Command, and Lt. Gen. Lincoln D. Faurer, who had replaced Inman as NSA Director in March, finally allowed the action to proceed.³⁴⁶

Marsh and Faurer did not settle the matter at their meeting but their mutual decision that the issue would be resolved provided sufficient motivation for their respective staffs to reach some accommodation. Ultimately, two changes were required in the directive in order to obtain the Air Force's concurrence. This agreement, however, was only informally conveyed. Walker was hesitant to proceed

without formal Air Force agreement since the official record included a formal non-concurrence. When it became apparent that the formal agreement was not forthcoming, Walker's superior, Under Secretary of Defense for C³I Donald C. Latham, took it upon himself to forward the directive for signature.³⁴⁷ The directive was finally signed on October 25, 1982, granting an official charter (Appendix C) to the Computer Security Evaluation Center at NSA.³⁴⁸

Meanwhile, on August 10, 1981, Inman, now a full Admiral and Deputy Director of Central Intelligence, publicly announced the establishment of the new computer security center at NSA. Significantly, in light of his new responsibilities, he stated that the center was established "for the Department of Defense and the Intelligence Community" (emphasis added).³⁴⁹

This deliberate broadening of the center's charter to include the entire intelligence community should probably not be viewed as surprising. Although the CIA had been involved in computer security very early,³⁵⁰ it had never sought leadership in the COMPUSEC field. In fact, even when encouraged to take a more active role, the CIA demurred. In 1976 the staff of the Senate's Government Operations Committee attempted to extract from the CIA advice on how "other Federal departments could strengthen their own computer security safeguards." The staff's report states:

In response to the staff's request, [CIA] Director [George C.] Bush made clear that he did not consider it desirable for other agencies to look at the CIA for leadership in the computer security field. ". . . the agency cannot for obvious reasons discuss in detail the security methods used to safeguard computer operations," Bush said, adding, ". . . Each department and agency . . . must make its own judgment in this regard."³⁵¹

In the intelligence business, 'tis better to receive than to give.

Amidst this flurry of action within the national security sector, the civil sector of the government was also becoming sensitized to the need for computer security. Much of the civil sector's concern grew out of the same political environment that helped to spawn public cryptography. As Donald A. Marchand writes:

The outcome of the National Data Center controversy pointed out that the problems of privacy presented by any proposed computerized information system had to be acknowledged or the system would be the subject of public concern.³⁵²

It was this "public concern" that led to the passage of the Federal Privacy Act in 1974, which in turn heightened the attention given computer security within the civil sector. The Privacy Act provided that any government agency or government contractor that kept systems of records containing personal identifier data was required to protect those data from disclosure or compromise. It specified a fine of \$5000 for each violating disclosure. The act further required the Office of Management and Budget (OMB) to develop guidelines and regulations to help federal agencies comply and also to provide continuing assistance and oversight of the act's provisions.³⁵³

In July 1978 the OMB issued a policy memorandum that made the head of each agency responsible for "assuring an adequate level of security for all agency data whether processed in-house or commercially." It explicitly included "sensitive data not subject to national security regulations" as well as data that were. And it mandated the establishment of a formal computer security program in all federal agencies, including periodic audits and recertification of security safeguards. The memorandum further assigned specific responsibilities to the Department of Commerce (DoC), the General Services Administration (GSA), and the Civil Service Commission (CSC).

To the DoC it assigned the technical task of developing and issuing security standards and guidelines. The GSA was given the management task of assuring that government purchase requests for any and all procurable ADP items were consistent with applicable security standards and guidelines. The CSC (now called the Office of Personnel Management) was charged with the administrative task of establishing personnel security policies for federal personnel with ADP access.³⁵⁴

This memorandum was a remarkable government document. It was reasonably short, strongly and explicitly worded, and apparently contained few loopholes. Moreover, it required the submission of written plans for compliance. The DoC, the GSA, and the CSC were each given 60 days to submit plans for the execution of their respective responsibilities and each department and agency was given 120 days to develop a plan for implementing the mandated security program within its organization.³⁵⁵

To review the computer security plans submitted by the agencies the OMB created a four-person task force, which met in December 1978. The task force noted "substantial differences" in the way various agencies had interpreted the memorandum's requirements and decided that further clarification was needed. To aid in uniformity of submissions the task force developed a checklist, which it sent out in early 1979. Agencies were asked to resubmit their plans, using the checklist, by 28 February. That done, the task force disbanded.³⁵⁶

A second team was assembled to evaluate the new plans but, as it turned out, the job fell to a single individual who completed the evaluations in late 1979.³⁵⁷

One month later, on January 9, 1980, the OMB reorganized. It created a new Office of Regulatory and Information Policy comprised of three divisions, each responsible for a certain set of government agencies. The new office established "desk officers" for each agency, who were to become familiar with their particular agency's operation but many of whom admittedly were inexperienced in ADP, much less computer security.³⁵⁸

On December 11, 1980, President Carter signed Public Law 96-511, the Paperwork Reduction Act of 1980. The act was based on recommendations of the Commission on Federal Paperwork, the President's Federal Data Processing Reorganization Project, and the GAO, all of whom had advocated a stronger role for the OMB in information management.³⁵⁹ Among other responsibilities, the act charges the Director of the OMB with

developing and implementing policies, principles, standards, and guidelines on . . . safeguarding the security of information collected or maintained by or on behalf of agencies;

and

providing agencies with advice and guidance about information security, restriction, exchange, and disclosure.
...³⁶⁰

The act further provides for the establishment, within the OMB, of an Office of Information and Regulatory Affairs and specifies that the authority to administer all functions required by the act shall be delegated to the administrator of this new office.³⁶¹ Although this new office was promptly established, its creation represented little in the way of immediate organization change within the OMB. The establishment of the Office of Regulatory and Information Policy had apparently been partly in anticipation of the new law.

It would be very misleading to leave the impression that one of the principal purposes of the Paperwork Reduction Act was to improve computer security within the government. It is not even clear from the record that COMPUSEC, as such, so much as crossed the minds of the members of the Congressional committee that sponsored the legislation. In the 55-page report to accompany the original House bill, aside from the words in the act itself, there is not a single specific mention of computer security or of information security.³⁶² However, the act can certainly be interpreted as mandating a rather vigorous program in COMPUSEC within the U.S. government and, as will become clear in Chapter 7, the GAO, for one, chooses to interpret it in this way.³⁶³

The act did not breeze through the Congress. It was held up for months by a DoD objection that, as originally drafted, the act would further impede the Pentagon's acquisition of new computer equipment.³⁶⁴ As eventually passed, the act excluded all ADP equipment used for military or intelligence functions except that used in "routine administrative and business applications."³⁶⁵ Some have suggested that had other federal departments read the Paperwork Reduction Act as carefully as the DoD apparently did, the act might have encountered far more trouble. As one writer put it, "Most of the agencies blinked at the Paperwork Reduction Act, and it passed."³⁶⁶

When the law was passed, a clear division already appeared to exist between the computer security efforts of the civil and of the national security sides of government. Public Law 96-511, although it did not establish this division, certainly did nothing to weaken it and even appeared to ratify it. This could simultaneously have both good and bad effects.

On the one hand, by maintaining the separation the act offered the national security community the continued freedom to grapple with its own problems and to pursue its own technical and administrative solutions without being restrained by the pace or deterred by the enormous additional problems of the civil agencies. On the other hand, the act may have condemned the civil side of the government to several more years of groping for technical solutions on its own (assuming that its environment will even permit solutions), and did nothing to expedite the transfer of national security sector-developed mechanisms to the computers of the civil agencies.

NOTES for Part II -- Historical Background

1. U.S., Army Security Agency, Historical Background of the Signal Security Agency, Volume II, World War I, prepared under the direction of the Assistant Chief of Staff, G-2, 12 April 1946 (SRH-001), p. 1.
2. Ibid., p. 2.
3. Ibid., pp. 2-3.
4. Lambros D. Callimahos, "The Legendary William F. Friedman" (SRH-058), p. 7, n. 4.
5. Ibid.; Ronald Clark, The Man Who Broke Purple (Boston: Little Brown and Company, 1977), pp. 24, 27-31.
6. W.F. Friedman, Six Lectures on Cryptography (also referred to as The Friedman Lectures) (SRH-004), April 1963, p. 106; and Clark, Purple, p. 40.
7. Clark, Purple, p. 43.
8. The Origin and Development of the Army Security Agency 1917-1947 (Laguna Hills, Calif.: Aegean Park Press, 1978), pp. 3-5.
9. The American Black Chamber was the title of a book about the Cipher Bureau, written by Herbert O. Yardley in 1931 and published by the Bobbs-Merrill Company.
10. Origin and Development, p. 5.
11. See below, p. II-19.
12. Friedman, Lectures, p. 125.
13. Friedman, Lectures, p. 145.
14. David Kahn, The Codebreakers: The Story of Secret Writing (New York: The MacMillan Company, 1967), p. 325.
15. Ibid.
16. Ibid., p. 195.
17. Friedman, Lectures, pp. 145-147. See also Kahn, Codebreakers, p. 325, and U.S., Background, Vol. III, p. 240.
18. Friedman, Lectures, p. 143.
19. U.S., Background, Vol III, pp. 240-241.
20. Friedman, Lectures, pp. 148-149.

21. Ibid., p. 163.
22. U.S., Background, Vol. II, p. 47.
23. M.D. Fagan, ed., A History of Engineering and Science in the Bell System: The Early Years (1875-1925), Bell Telephone Laboratories, Inc. 1975, p. 755.
24. R.D. Parker, "Recollections Concerning the Birth of One-Time Tape and Printing-Telegraph Machine Cryptography" (SRQ-02), p. 110.
25. Fagan, Bell History (1875-1925), p. 755.
26. Parker, "Recollections," p. 111.
27. Howard E. Rosenblum, former Deputy Director for Communications Security, National Security Agency, in a letter to Anthony G. Oettinger, 13 June 1984.
28. Kahn, Codebreakers, pp. 397-398.
29. U.S., Background, Vol II, p. 53.
30. Friedman, Lectures, pp. 168-169.
31. Kahn, Codebreakers, pp. 401-402.
32. Ibid.
33. W. Diffie and M.E. Hellman, "Privacy and Authentication: An Introduction to Cryptography" Proceedings of the IEEE 67 (March 1979):406.
34. All cryptographic equipments developed by the Army during this period were assigned short titles beginning with the letters "S-I-G." The three or four letters which were used to fill out the designator were assigned arbitrarily. (Source: Interview with Howard Barlow, former Assistant Director for Communications Security, National Security Agency on 16 December 1981.)
35. Clark, Purple, p. 94.
36. Diffie and Hellman.
37. Dorothy Elizabeth Robling Denning, Cryptography and Data Security (Reading, Mass.: Addison-Wesley Publishing Company, 1982), p. 85.
38. Kahn, Codebreakers, pp. 415-417.
39. Clark, Purple, p. 95.
40. Ibid., p. 96.

41. Kahn, Codebreakers, p. 418; Howard Barlow, personal correspondence dated 27 September 1983.
42. Clark, Purple, p. 96.
43. For a detailed account of the rather poignant story of Hebern's difficulties, see Kahn, Codebreakers, pp. 415-420.
44. Clark, Purple, p. 134.
45. U.S., Background, Vol. III, p. 251-252.
46. Clark, Purple, p. 195-196.
47. U.S., Background, Vol. III, p. 241.
48. Ibid., pp. 241-250.
49. Ibid., p. 242.
50. Ibid., p. 243.
51. Ibid.
52. A letter, dated August 3, 1937 and signed by Colonel William R. Blair of the Laboratories specifically stated, "Active work on project 6-a [the M-161] was not started until completion of the Converter M-134-C." (See U.S., History Vol. III, p. 247). Obviously, different parts of the same Army were not talking to one another.
53. U.S., Background Vol. III, p. 245.
54. Ibid., p. 245.
55. Ibid., p. 246.
56. Ibid., p. 248.
57. Ibid., p. 249.
58. This assumption is a consequence of the basic distinction between the general system and the specific key. According to Gordon Welchman, the first person to make this distinction explicit was August Kerckhoffs in his book, La Cryptographie Militaire, published in 1883. According to Welchman, "he foresaw that if a general system were to be used by too many individuals it would inevitably be compromised, and that secrecy should reside solely in the particular key, which could be changed at will." Thus Kerckhoffs introduced, nearly a century ago, what nowadays is sometimes called the fundamental assumption of military cryptography: that the enemy knows the general system. See Gordon Welchman, The Hut Six Story:

Breaking the Enigma Codes (New York: McGraw-Hill Book Company, 1982), pp. 25-26.

59. U.S., Background, Vol. III, p. 250.
60. Ibid.
61. Kahn, Codebreakers, p. 427.
62. U.S., Background, Vol. III, p. 250.
63. Kahn, Codebreakers, p. 427.
64. Ibid.
65. Ibid.
66. Clark, Purple, p. 149.
67. Denning, Cryptography, p. 85.
68. Ibid.
69. Friedman, Lectures, p. 169.
70. M.D. Fagan (ed.), A History of Engineering and Science in the Bell System: National Service in War and Peace (1925-1975), Bell Telephone Laboratories, Inc., 1978, p. 296.

Among those who worked on the X System at Bell Labs were Alan Turing, the British mathematician famous for his cryptanalytic work on the German ENIGMA and for whom the "Turing Machine" is named, and Claude E. Shannon of Bell Labs, whose 1940 treatise on "Communication in the Presence of Noise" marked the beginning of the formal study of information theory. (See Andrew Hodges, Alan Turing: The Enigma (New York: Simon and Schuster, 1983), pp. 246-250.)

71. Ibid., p. 298.
72. Ibid., p. 292.
73. Fagan, Bell History (1875-1925), p. 420.
74. Fagan, Bell History (1925-1975), p. 294.
75. Ibid., p. 295.
76. Ibid., pp. 298-299.

In the SIGSALY, the frequency spectrum of a speech wave is first divided into ten very equal bands between 150 Hz and 2950 Hz. Each band is then limited to 25 Hz by low-pass filtering. A determination is made as to whether the sound is voiced or

unvoiced. If voiced, the pitch or fundamental frequency is measured to constitute an eleventh channel of information. Each channel is quantized to one of six levels except the pitch channel which, by using a vernier method and two output channels, achieves a 36-level quantization. The twelve resultant output channels of six-level information are then combined with key, also of six levels, stored on phonograph records. The combination is performed as in non-carry or modulo-6 addition, yielding again twelve six-level channels. These in turn are fed into individual FM modulators. The output signal, therefore, consists of twelve parallel frequency shift keyed (FSK) channels. See Ibid., pp. 299-306.

77. The National Defense Research Committee, established by President Franklin D. Roosevelt on June 27, 1940, was composed of scientists from industry, academic circles, and the military. See Fagan, Bell History (1925-1975), pp. 7-8.
78. This is the same Joseph O. Mauborgne mentioned earlier as a Major. See above, p. II-5.
79. Fagan, Bell History (1925-1975), p. 310.
80. Ibid., pp. 311-312.
81. Ibid., p. 315.
82. Interview with Roland O. Laine, retiree from the National Security Agency on 11 November 1982.
83. Interview, Barlow.
84. Ibid.
85. Kahn, Codebreakers, p. 710. The word "principles" in this quotation should more properly read "devices." The literal encipherment principles upon which these later devices were based can actually be traced to professional cryptographers of the middle ages -- particularly those in the employ of the Vatican. See Kahn, Codebreakers, Chapters 3 and 4.
86. Kahn, Codebreakers, p. 709.
87. Actually, this monopoly has never been total. In spite of directives that appear to mandate otherwise, many government agencies have always seemed to feel free to satisfy at least some of their COMSEC needs directly -- without recourse to the NSA.
88. Origin and Development, pp. 3-5.
89. Ibid., p. 6.
90. Ibid.

91. Clark, Purple, pp. 64-65, 70-72, 78-79.
92. James Bamford, The Puzzle Palace (Boston: Houghton Mifflin Company, 1982), p. 33.
93. According to Bamford (ibid.), the designation OP-20-G, "meant that it was G Section (Communications Security) of the 20th Division (Office of Naval Communications) of the Office of Chief of Naval Operations (OP)."
94. U.S., Report to the Secretary of State and the Secretary of Defense (commonly referred to as the Brownell Committee Report), 13 June 1952, p. 4.
95. William F. Friedman, "A Brief History of the Signal Intelligence Service" (SRH-029), 29 June 1942, p. 14.
96. U.S., Background Vol. III, pp. 140-142.
97. Origin and Development, p. 7.
98. U.S., Background Vol. III, p. 180.
99. Origin and Development, p. 8. See also ibid., p. 182.
100. Bamford, Puzzle Palace, p. 16.
101. Origin and Development, p. 8.
102. Ibid., pp. 11-12.
103. Ibid., p. 33.
104. The MIT Radar School was started on June 23, 1941. The program at Harvard was begun only a few weeks later on July 17, 1941. Although the schools were separate, there was a close liaison between them with "curriculum coordination conferences" held frequently. Later, programs similar to Harvard's were established at Bowdoin College and at Princeton University. By the war's end, MIT had counted 8,657 students as having passed through their school. See W.H. Radford, "Technology's Radar School," Technology Review, February 1946, pp. 227-250; John Burchard, Q.E.D.: MIT in World War II (New York: John Wiley & Sons, Inc., 1948), pp. 226-228.
105. Interview with William P. King, retiree from the National Security Agency on 28 October 1982.
106. Ibid.
107. Kahn, Codebreakers, pp. 678-679.
108. Origin and Development, p. 38.

109. U.S., Brownell Committee Report, p. 47.
110. Ibid., p. 102.
111. Ibid., pp. 20-21.
112. Interview, Barlow.
113. Bamford, Puzzle Palace, p. 52. See also U.S., Brownell Committee Report, particularly the covering letter and Exhibit A-1.
114. U.S., Brownell Committee Report, pp. 118-120.
115. Interview, Barlow.
116. U.S., Brownell Committee Report, p. 6 of the covering letter.
117. Ibid., p. 101.
118. Ibid., p. 102.
119. Bamford, Puzzle Palace, p. 55.
120. ULTRA was the codename assigned to the intelligence derived from the decryption of the German cipher machine, ENIGMA; MAGIC was the codename associated with the signals intelligence derived from the Japanese PURPLE machine.
121. Soon after the war ended, in the fall of 1945, and several years before AFSA was formed, research and development was organized as a separate activity within the Army Security Agency. The new research and development organization supported both the intelligence and the COMSEC missions of the new agency. (Barlow interview.)
122. Interview, Barlow.
123. Solomon Kullback was one of three mathematicians whom Friedman hired as "junior cryptanalysts" in 1930, shortly after the Signals Intelligence service was created. The other two were Frank B. Rowlett and Abraham Sinkov. See U.S., Historical Background Vol. III, p. 203; and Bamford, Puzzle Palace, p. 30.
124. Interview, Barlow.
125. Interview with Thomas Witcher, Chief, COMSEC Procurement and Acquisition, National Security Agency on 8 December 1982.
126. Interview, Barlow.
127. Bamford, Puzzle Palace, p. 98-99.
128. Interview, Barlow.

129. Ibid.
130. Interview, King.
131. Interview, Witcher.
132. Ibid.
133. Interview, Barlow.
134. The patent was applied to a high-speed computer printer. "The Agency wanted a high-speed printer for its own computer output and the best anybody had at the time was a Teletype." The patented machine, which substituted a magnetic pickup head for a complex arrangement of "cams and contacts" as the print triggering device, raised the achievable print speeds from approximately 4.5 seconds per line to 10 lines per second. (Barlow interview.)
135. Interview, Witcher.
136. Ibid.
137. Ibid.
138. Ibid.
139. Interview, Barlow.
140. Ibid.
141. Interview, Witcher.
142. Interview, Laine.
143. Ibid.
144. Interview, Barlow.
145. Above, pp. II-15 to II-17.
146. Pulse Code Modulation (PCM) consists of three steps. First, the speech is scanned at a suitable rate and the amplitude measured at each time interval. Second, the amplitudes are quantized to a nearest integer value. Third, these integers are coded in ordinary telegraphic code. See E. Maurice Deloraine and Alec H. Reeves, "The 25th anniversary of pulse code modulation," IEEE Spectrum 5 (May 1965):57.
147. Fagan, Bell History 1525-1975, p. 316.
148. Interview, Barlow.
149. Interview, Laine.

150. Interview, Barlow.
151. Mathews was later to serve as head of NSA's R&D organization. See Bamford, Puzzle Palace, p. 97.
152. Interview, Laine.
153. Above, pp. II-11 to II-13.
154. Interview, Barlow.
155. Delta modulation differs from PCM in that it makes use of past information about the input signal. In its most basic form, the delta modulation process can be thought of as an approximation of the input signal with a staircase signal whose every step is of the same size. At each sampling point, the approximating (staircase) signal must move exactly one step up or down, all the while trying to match the input signal as closely as possible. The output (delta modulated) signal, then, represents this staircase signal by outputting a "1" if the staircase steps up and a "0" if the staircase steps down. See Martin S. Roden, Analog and Digital Communications Systems (Englewood Cliffs, N.J.: Prentice-Hall, Inc., 1979), pp. 283-285.
156. Interview, King.
157. Interview, Barlow.
158. Ibid.
159. Interview, King.
160. Ibid.
161. Ibid.
162. Ibid.
163. Ibid.
164. Ibid.
165. Ibid.
166. Transistors are composed of two basic kinds of semiconductor materials, with one of the two materials sandwiched between layers of the other. One of the two materials, called P-type, contains a relative shortage of electrons, while the other, called N-type, has a relative surplus of electrons. When voltage is applied in the proper direction, electrons are able to flow across the boundary between the layers. Semiconductor materials are crystals and the relative shortage or surplus of electrons is obtained by deliberately contaminating an electrically neutral and stable crystal like silicon with gases

that possess the desired chemical property. A PNP transistor has a layer of N-type material between two layers of P-type, whereas an NPN transistor has a layer of P-type between layers of N-type.

167. Interview, King.
168. Rosenblum, Letter to Oettinger.
169. Cf., for example, Raymond Tate, "Worldwide C³I and Telecommunications," Seminar on Command, Control, Communications and Intelligence, Program on Information Resources Policy, Harvard University, Cambridge, Mass., Incidental Paper I-80-6, December 1980, p. 41; John H. Cushman, "C³I and the Commander: Responsibility and Accountability," Seminar on Command, Control, Communications and Intelligence, Program on Information Resources Policy, Harvard University, Cambridge, Mass., Incidental Paper I-81-9, December 1981, pp. 114-117; and Richard G. Stilwell, "Policy and National Command," Seminar on Command, Control, Communications and Intelligence, Program on Information Resources Policy, Harvard University, Cambridge, Mass., Incidental Paper I-82-3, December 1982, p. 145.
170. Interview, Laine.
171. Interview, Barlow.
172. Interview, Laine.
173. Interview, King.
174. Interview, Laine.
175. Interview, Barlow.
176. Ibid.
177. Ibid.
178. Ibid.
179. Interview, Laine.
180. Interview, Barlow.
181. Interview, Laine.
182. Ibid.
183. Ibid.
184. Interview, Barlow.
185. Ibid.

186. Ibid.
187. Interview, King.
188. Barry Miller, "SSD Plans Space Test of Unified Avionics," Aviation Week & Space Technology, 30 November 1964, p. 42.
189. Interview, King.
190. Ibid.
191. J. Michael Nye, "Cryptography Market: Products, Costs, Trends," Telecommunications, April 1982, p. 80.
192. For a discussion of the National Data Center, see James Rule, Douglas McAdam, Linda Stearns, and David Uglow, The Politics of Privacy (New York: The New American Library, Inc., 1980), pp. 55-57.
193. Refer to an excerpt from a Senate speech by Senator Sam Ervin on 11 June 1974 contained in U.S., Congress, Senate, Government Operations Committee, Legislative History P.L. 93-579: Privacy Act of 1974, 93d Cong., 2d sess., 26 September 1974.
194. Louise E.G. Becker, Privacy: Information Technology Implications, Congressional Research Service Issue Brief Number IB 74105, updated 21 March 1975, pp. 1, 3.
195. David Kahn, "Cryptology Goes Public," Foreign Affairs 58 (Fall 1979):144.
196. Whitfield Diffie, NSA and the Independent Cryptographers -- An Uneasy Cooperation, BNR Inc., Mountain View, Calif., December 1981, p. 2.
197. Kahn, "Cryptology," p. 153.
198. Diffie, "Independent Cryptographers," p. 4.
199. Tom Ferguson, Private Locks, Public Keys and State Secrets: New Problems in Guarding Information with Cryptography, Program on Information Resources Policy, Harvard University, Cambridge, Mass., Publication No. P-82-5, April 1982, p. 18.
200. U.S., Congress, Senate, Select Committee on Intelligence, Unclassified Summary: Involvement of NSA in the Development of the Data Encryption Standard, 95th Cong., 2d sess., April 1978, p. 2.
201. Interview with Harry B. DeMaio, Director of Data Security Programs, IBM Corporation, on 17 August 1984.

The development of LUCIFER had a very long history that began not at IBM, but at the Air Force Cambridge Research Center

(AFCRC). During the 1950s a cryptographic research group was formed at the AFCRC under the leadership of Horst Feistel. According to a member of the original group, Peter Schweitzer, the group consisted of some six mathematicians plus three consultants, two of whom spent one day a week on the project. In search of a reliable means of distinguishing friendly from non-friendly aircraft, the group worked mainly on the designs and analysis of methods of block encipherment. Although, according to Schweitzer, the group's work was "closely coordinated with NSA," the effort "did not, for quite some time, seriously involve any of their really good people." A breadboard version was eventually produced by the AFCRC, which Schweitzer believes may have been the first all-transistor cryptographic device. (cf. p. II-36). The AFCRC group eventually disbanded and, after a few brief jobs with some Air Force contractors, Feistel found himself at IBM where he was able to convince his management of the need for some encryption scheme to protect the rapidly increasing communications among computers. (See Peter Schweitzer, letter to Anthony Oettinger, dated 26 June 1984). Although at IBM Feistel worked under Walter Tuchman who himself made important contributions to LUCIFER and later to the DES, the IBM Corporation still considers Horst Feistel "the algorithmic father of DES." (DeMaio interview.)

202. Ferguson, Private Locks, p. 18.
203. Sylvia Sanders, "Data Privacy: What Washington Doesn't Want You to Know," REASON, January 1981, p. 31.
204. Gina Bari Kolata, "Computer Encryption and the National Security Agency Connection," Science, 29 July 1977, p. 197.
205. U.S., Congress, Unclassified Summary, p. 4.

A cryptographic machine derives its strength from the combination of the algorithm, the mathematical operations performed by the machine, and the keying variable, sometimes called the variable or the key, which specifies the initial condition or setting of the device. Normally, the algorithm does not change. All machines of the same type embody the same algorithm. Additionally, however, in order to communicate with one another, they must be placed in the same initial state. This is done by way of the keying variable. Thus, in order for an unintended recipient or eavesdropper, to decipher or break back a message, he must correctly guess or otherwise determine the correct keying variable. The greater the number of possible variables, the longer it is likely to take to find the correct one. Typically, the keying variable is expressed as a string of digits. The longer this string, the greater the set of possible variables and the greater the potential security of the device. The variable size of the DES is 56 binary digits. Therefore, there are 2^{56} , or approximately 72 quadrillion, possible variables from which to select one.

206. M. Blake Greenlee, as quoted in Gina Bari Kolata, "Computer Encryption and the National Security Agency Connection," Science 197 (29 July 1977):440.
207. Robert Morris, in a Letter to the Editor, Science 197 (19 August 1977):716.
208. Whitfield Diffie and Martin E. Hellman, "New Directions in Cryptography," IEEE Transactions on Information Theory IT-22 (November 1976):644-654.
209. Abraham Lempel, "Cryptology in Transition," ACM Computing Surveys 11 (December 1979):287.
210. Michael Willett, "A Tutorial on Public Key Cryptography," Computers & Security 1 (January 1982):73.
211. For an in-depth discussion of public key cryptography and of several of the proposed implementing schemes, see Lempel, "Cryptology," pp. 294-299; Willet, "A Tutorial," pp. 73-77; and Dorothy Elizabeth Robing Denning, Cryptography and Data Security (Reading, Mass.: Addison-Wesley Publishing Company, 1982), pp. 11-14, 101-126.
212. Diffie, "Independent Cryptographers," p. 7.
213. David Kahn, "The Public's Secrets," Cryptologia 5 (January 1981):23.
214. Diffie, "Independent Cryptographers," p. 7.
215. Becker, Privacy, p. 3.
216. Donald E. Kraft and Charles K. Wilk, "Emerging Federal Government Actions in Telecommunications Protections," Proceedings of the National Electronics Conference, XXXIII (Oak Brook, Ill.: National Engineering Consortium Inc., October 1979), p. 315.
217. David Burnham, "Carter Approves Plan to Combat Phone Spying by Other Nations," The New York Times, 20 November 1977, sec. 1, p. 34.
218. These deliberations apparently grew out of a special panel of the National Security Council that began in 1974 and was headed by Edward E. David, Jr., who was then science advisor to President Nixon. See Greg Lipscomb, Private and Public Defenses Against Soviet Interception of U.S. Telecommunications: Problems and Policy Points, Program on Information Resources Policy, Harvard University, Cambridge, Mass., Publication P-79-3, July 1979, p. 7.
219. David Burnham, "New Unit Seeks to Prevent Russians from Spying on U.S. Phone System," New York Times, 26 March 1979, p. A16.

220. Interview with former member, Office of Telecommunications Policy OTP on 16 December 1982.
221. Ibid.
222. Lipscomb, Private and Public Defenses, p. 62.
223. Ibid., pp. 63-64. See also Ferguson, Private Locks, p. 62.
224. Interview with Donald E. Kraft, National Communications System, formerly with Special Projects Office, National Telecommunications and Information Administration (NTIA) on 29 October 1982.
225. Burnham, "Carter Approves Plan," p. 34.
226. B.R. Inman, from text of remarks in "Issues in Intelligence," Seminar on Command Control, Communications and Intelligence: Guest Presentations--Spring 1981, Program on Information Resources Policy, Harvard University, Cambridge, Mass., Incidental Paper I-81-9, December 1981, p. 211.
227. Interview with Admiral Bobby R. Inman, USN (ret.), former Director, National Security Agency on 16 December 1982.
228. Interview, Kraft.
229. Burnham, "Carter Approves Plan," p. 34.
230. Kraft and Wilk, "Emerging Actions," p. 315.
231. NTIA was created in March 1978 by E.O. 12046 as part of President Carter's Reorganization Plan.
232. Alan Pearce, "NTIA -- Washington's Latest Bureaucracy," Telecommunications, June 1978, p. 102.
233. Burnham, "New Unit," p. A16.
234. Interview, former member, OTP.
235. Interview, Kraft.
236. Kraft and Wilk, "Emerging Actions," p. 315.
237. Ibid.
238. Interview with Charles K. Wilk, National Telecommunications and Information Administration (NTIA) on 29 October 1982.
239. Among the studies funded by NTIA were: Impact Evaluation of Selected National Policy Alternatives on Private Sector Research in Cryptography for Telecommunications Protection, dated 31 May 1981, and performed by CRC Systems, Inc.; Impacts of Federal

Policy Options for Non-military Cryptography, dated April 1981 and prepared by SRI International; and Users' Guide: Voice and Data Communications Protection Equipment, dated December 1980 and prepared by J. Michael Nye of Marketing Consultants International, Inc. To gain an insight into the scope of the course, see U.S., Dept. of Commerce, National Telecommunications and Information Administration, Telecommunications Protection Training Program: Student Reference Guide.

240. Interview, Kraft.
241. Interview, Wilk.
242. Henry Geller, former Assistant Secretary for Communications and Information, Department of Commerce, in a letter to Anthony G. Oettinger dated 17 September 1984.
243. A second, less specific, source of authority for the NTIA's communications protection mission can be found in Executive Order 12046, dated 27 March 1978. Section 2-405 of that E.O. reads:
- 2-405. The Secretary of Commerce shall provide for the coordination of the telecommunications activities of the Executive Branch, and shall assist in the formulation of policies and standards for those activities, including but not limited to considerations of interoperability, privacy, security, spectrum use and emergency readiness. (emphasis added)
244. Interview with Robert C. Massey, Survey and Training Branch, Special Project Office, National Telecommunications and Information Administration on 29 October 1982.
245. Interview, Wilk.
246. Interview, Massey.
247. U.S., General Accounting Office, Increasing Use of Data Telecommunications Calls for Stronger Protection and Improved Economies (LCD-81-1), 12 November 1980, p. 17.
248. Ibid., p. 18.
249. Geller, letter to Oettinger.
250. Interview, Wilk.
251. Ibid.
252. Interview, Massey.
253. Interview with James H. Burrows, Director, Institute for

Computer Sciences and Technology, National Bureau of Standards
on 1 September 1982.

- 254. Interview with a DoD official on 29 August 1982.
- 255. Interview, Inman.
- 256. Geller, letter to Oettinger.
- 257. Interview, Wilk.
- 258. Ibid.
- 259. Interview, Inman.
- 260. Ibid.
- 261. B.R. Inman, "The NSA Perspective on Telecommunications Protection in the Nongovernment Sector," text of a talk presented at the AFCEA Vital Telecommunications Issues Symposium and reprinted in Signal, March 1979, p. 6.
- 262. Deborah Shapley, "Intelligence Agency Chief Seeks 'Dialogue' with Academics," Science, 27 (October 1978):407-410 and ibid., pp. 6-13.
- 263. Among the other factors that caused Inman to go public were growing differences over the issue of public cryptography between NSA and some members of the academic community -- notably Martin Hellman of Stanford and George Davida of the University of Wisconsin -- and internal NSA concerns about what it perceived as "one-sided coverage" by the scientific and public media. (B.R. Inman, personal communications, 29 June 1983).
- 264. Interview, Inman.
- 265. Ibid.
- 266. Inman, "Issues in Intelligence," pp. 211-212.
- 267. "Cutting into NTIA's Cuts," Broadcasting, 29 March 1982, p. 118.
- 268. Willie Schatz, "NTIA Stakes Its Turf," Datamation, September 1981, p. 100.
- 269. Interview with Harold J. Podell, Mission Analysis and Systems Acquisition Division, General Accounting Office on 31 August 1982. (Note: Dr. Podell's views do not necessarily reflect the views of the General Accounting Office.)
- 270. Interview, Massey.
- 271. Raymond Tate, former Deputy Director for Communications

- Security, National Security Agency, private correspondence dated October 1984.
272. Ferguson, Private Locks, p. 18.
 273. Interview, Burrows.
 274. U.S., Congress, Senate, Committee on Government Operations, Staff Study of Computer Security in Federal Programs, 95th Cong., 1st sess., February 1977, p. 138.
 275. J. Michael Williams, Systems Development Corporation, personal correspondence; Carl E. Landwehr, "The Best Available Technologies for Computer Security," Computer, July 1983, pp. 90, 96.
 276. Eugene V. Epperly, "The Department of Defense Computer Security Initiative Program and Current and Future Computer Security Policies," Proceedings of the Second Seminar on the DoD Computer Security Initiative Program, National Bureau of Standards, Gaithersburg, Md., January 15-17, 1980, p. J-3.
 277. Willis H. Ware (ed.), Security Controls for Computer Systems, Report of Defense Science Board Task Force on Computer Security, The Rand Corporation Report R609-1, Reissued October 1979, pp. vii-viii.
 278. Ibid., p. iii.
 279. U.S., Congress, Staff Study, p. 156.
 280. U.S., Department of Defense, "Security Requirements for Automatic Data Processing (ADP) Systems," Dept. of Defense Directive Number 5200.28, Change #2, 29 April 1978, p. 9.
 281. Interview with Stephen T. Walker, former Director, Information Systems, Office of the Deputy Under Secretary of Defense Research and Engineering (C²I) on 31 August 1982.
 282. Stephen T. Walker, "The Advent of Trusted Computer Operating Systems", AFIPS Conference Proceedings 1980 National Computer Conference, Anaheim, Calif., May 19-22, 1980 (Arlington, Va.: AFIPS Press, 1980), p. 655.
 283. MULTICS, for Multiplexed Information and Computing Service, was an operating system for the GE645 computer, developed by Honeywell Information Systems, with DoD sponsorship. An earlier GE computer used by the Air Force had been successfully penetrated by a Tiger team and found to be "not only insecure but insecurable." The Honeywell development was intended to make substantial improvements in several areas, including security. However, the resulting MULTICS system was also successfully penetrated and as each penetration was blocked, a new penetration was discovered. In at least one case, the

penetration took advantage of a flaw that resulted from changes made to correct previous ones. The government eventually concluded that developing a multilevel computer through a series of improvements was going to be difficult, if not futile. See Roger R. Schell, "Computer Security: The Achilles Heel of the Electronic Air Force?" Air University Review, XXX (January-February 1979):21-23.

284. Loring Wirbel, "Somebody is Listening", The Progressive, November 1980, p. 21.
285. D.E.R. Denning, Cryptography and Data Security (Reading, Mass.: Addison-Wesley Publishing Company, 1982), p. 318. Actually, the Denning statement is probably unnecessarily restricted. To the author's knowledge, the statement would be equally true if it began, "Prior to the 1980's," The only commercial product known to have withstood concerted attempts at penetration is the Honeywell SCOMP. (See pp. III-30, 31.)

"Multilevel," as used here and throughout this paper, has a very specific (but imprecise) meaning. It refers to one of two DoD authorized modes of operation of an ADP system that permit use of the system by individuals who are not "cleared" for all the information within the system. The second mode that permits the same thing is called the "controlled" mode. The distinction between them is that the controlled mode relies on security controls external to the computer's operating system whereas, in the multilevel mode protection is afforded by the operating system itself. See U.S., Department of Defense, "Security Requirements for Automatic Data Processing (ADP) Systems," DoD Directive 5200.28 Change 2, 29 April 1978. The imprecision of the term arises from the fact that it could be used to describe systems of two levels, e.g. confidential and secret, as well as systems of ten or more levels, embracing all classifications and several special access categories.

286. U.S., Air Force, Electronic Systems Division (AFSC), ESD 1974 Computer Security Development Summary, Interim Report MCI-75-1, 31 December 1974, p. 7.
287. Philip A. Myers, "Subversion: The Neglected Aspect of Computer Security", Masters Thesis, Naval Postgraduate School, Monterey, Calif., June 1980, p. 14.
288. Denning, p. 318.
289. U.S., ESD Summary, p. 8.
290. Ibid.
291. James P. Anderson, Computer Security Technology Planning Study, ESD-TR-73-51, Vol. I, October 1972, p. 21.
292. Ibid., p. iv.

293. U.S., ESD Summary, p. 9.
294. Ibid., p. 11. See also Stanley R. Ames, Jr., Morrie Gasser, and Roger R. Schell, "Security Kernel Design and Implementation: An Introduction," Computer, July 1983, p. 14.
295. Ibid., p. 9 and Anderson, Planning Study Vol. 1, pp. 9-10.
296. Walker, "Advent," p. 657.
297. Interview with Col. Roger R. Schell, Deputy Director, DoD Computer Security Evaluation Center, National Security Agency on 28 October 1982. Essentially the same idea is quoted in Ames et. al., "Kernel Design and Implementation," p. 15.
298. Walker, "Advent," pp. 655-656; see also J. Barton De Wolf and Paul A. Szulewski (eds.), Final Report of the 1979 Summer Study on Air Force Computer Security, The Charles Stark Draper Laboratory, Inc., Cambridge, Mass., October 1979, pp. 19-29.
299. Schell, "Achilles Heel," p. 33, n. 15.
300. Interview, Walker, 31 August 1982.
301. Telephone interview with Col. Roger R. Schell, Deputy Director, DoD Computer Security Center, National Security Agency on August 1982.
302. Interview, Schell, 28 October 1982.
303. Interview with Stephen T. Walker, former Director, Information Systems, Office of the Deputy Under Secretary of Defense Research and Engineering (C³I) on 28 October 1982.
304. Interview, Walker, 31 August 1982.
305. Ibid.
306. Ibid.
307. Interview, Walker, 28 October 1982.
308. James J. Croke, Vice President, Bedford Operations, The MITRE Corporation, personal correspondence dated 17 July 1984.
309. Ibid.
310. Proceedings of the Seminar on the DoD Computer Security Initiative Program, National Bureau of Standards, Gaithersburg, Md., 17-18 July, 1979, p. iii.
311. Interview, Walker, 31 August 1982.
312. Above, p. II-70.

- 313. Interview, Walker, 31 August 1982.
- 314. Interview, Walker, 28 October 1982.
- 315. Interview, Walker, 31 August 1982.
- 316. Interview, Walker, 28 October 1982.
- 317. Interview with Stephen T. Walker former Director, Information Systems, Office of the Deputy Under Secretary of Defense Research and Engineering (C³I) on 23 July 1982.
- 318. Ibid.
- 319. Ibid. For discussion of the NORAD computer failure, see U.S., Congress, House, Committee on Government Operations, NORAD Computer Systems are Dangerously Obsolete, 97th Cong., 2d sess., 1982, H. Rept. 449, pp. 3-4.
- 320. Above, pp. II-63 to II-65.
- 321. Ibid.
- 322. Ibid.
- 323. Interview, Walker, 31 August 1982.
- 324. Ibid.
- 325. Interview, Inman.
- 326. Ibid.
- 327. Ibid.
- 328. Ibid.
- 329. Ibid.
- 330. Ibid.
- 331. Ibid.
- 332. Ibid.
- 333. Interview, Walker, 31 August 1982.
- 334. Conversation with Walter G. Deeley, National Security Agency, on 17 December 1982.
- 335. Interview, Walker, 28 October 1982.
- 336. Ibid.

337. Ibid.
338. Ibid.
339. Ibid.
340. Memorandum, Subject: "DOD Computer Security Evaluation Center," signed by Deputy Secretary of Defense, W. Graham Claytor, Jr., dated 2 January 1981.
341. Interview, Walker, 28 October 1982.
342. Ibid.
343. Terence Hunt, "Reagan Plans Welcome for Returnees, Meets with Cabinet," Associated Press Release, 24 January 1981.
344. Interview, Walker, 28 October 1982.
345. Ibid.
346. Ibid.
347. Ibid.
348. U.S., Department of Defense, "Computer Security Evaluation Center," Dept. of Defense Directive Number 5215.1, 25 October 1982.
349. Bobby R. Inman, "Keynote Address: Computer Security Initiative," Proceedings of the Fourth Seminar on the DoD Computer Security Initiative, National Bureau of Standards, Gaithersburg, Md., 10-12 August 1981, p. B-2.
350. See p. II-68.
351. U.S., Congress, Staff Study, pp. 137-138.
352. Donald A. Marchand, The Politics of Privacy, Computers, and Criminal Justice Records (Arlington, Va.: Information Resources Press, 1980), pp. 123-124.
353. 5 USC 552a.
354. U.S., Executive Office of the President, Office of Management and Budget, "Security of Federal automated information systems" (Circular No. A-71, Transmittal Memorandum No. 1), 27 July 1978.
355. Ibid.
356. U.S., General Accounting Office, "Central Agencies' Compliance with OMB Circular A-71, Transmittal Memorandum No. 1," (LCD-80-56-I), 30 April 1980, p. 2.

- 357. Ibid.
- 358. Ibid., pp. 2-3.
- 359. U.S., Congress, House, Committee on Government Operations,
Paperwork Reduction Act of 1980: Report to Accompany H.R. 6410,
96th Cong., 2d sess., 1980, H. Rept. 835, p. 3.
- 360. 44 USC 3504.
- 361. 44 USC 3503.
- 362. U.S. Congress, Paperwork Reduction Act.
- 363. Below, pp. III-8, 9.
- 364. Richard L. Worsnop, "Trimming Federal Paperwork," Congressional
Quarterly, 23 March 1981.
- 365. 44 USC 3502.
- 366. Cecelia Wertz, "Paperwork Reduction," Administrative Law Review
34 (Spring 1982):156.

PART III

THE CURRENT CONDITION

Chapter 7

A Confusing Muddle

At the time that NSDD-145 was signed, the state of information security, inside and outside the government, was in somewhat of a muddle. Certainly, within the government there was no single organization that could claim overall responsibility for information security -- for policy formulation, for technical standards, for research and development, for production of mechanisms, for evaluation of systems and products, for managing procurement, for personnel security, or even for technical advice. Besides this division according to function, responsibility was also divided along civil-national security lines and along COMSEC-COMPUSEC lines. Thus, even the same function could be split four ways. The problem with this attempted division is that present teleprocessing systems elude such neat dissection. The difficulty that NTIA faced when it tried to define the difference between national security-related and non-national security-related information and then to apply that definition to individual systems has not abated.¹ If anything, it has grown worse. Nor is the attempted split between communications security and computer security any easier to define, as both policy and technical organizations are discovering.

Consider policy, for example. Before NSDD-145, COMSEC policy for the national security sector was the responsibility of the National Communications Security Committee (NCSC). The responsibility for computer security in the national security sector was not as clear. Within the DoD, it appeared to fall under the Office of the Deputy

Under Secretary of Defense for Policy [ODUSD (Policy)]. One would not expect a Deputy Under Secretary of Defense to exercise policy jurisdiction outside of the DoD, and apparently in computer security, he has not. According to a NCSC Working Group report, the basis for computer security within the intelligence community has been Director of Central Intelligence Directive No. 1/16 (DCID 1/16) issued by the DCI. The report notes, however, that DCID 1/16 specifically excludes "ADP systems and/or networks that are used exclusively for telecommunications services."²

On the civil side, communications protection policy, for other than classified information was officially assigned, during the Carter administration, to a Special Coordinating Committee (SCC) of the National Security Council. The SCC was to "exercise this responsibility through a special Subcommittee on Telecommunications Protection," which was chaired by the Director, Office of Science and Technology Policy, Dr. Frank Press.³ The SCC was chaired by then National Security Advisor Brzezinski.⁴ Computer security policy on the civil side was, by virtue of the Paperwork Reduction Act, the responsibility of the Office of Management and Budget.

Thus, policy was split at least four ways. All of this subdividing has not been without adverse consequences. Writing about the civil-national security split on the COMSEC side, a 1981 SRI report stated:

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 electronics and information systems.⁵

Even before the September 1984 directive, there were attempts to deal with some of the policy muddle. Within the national security sector, with respect to the COMSEC-COMPUSEC split, the NCSC in the late 1970s recognized that the security of the nation's communications was becoming increasingly dependent upon the security of various computers and processors. Yet the NCSC also realized that it lacked any clear charter in computer security. The NCSC fully understood that the OMB -- not itself -- had been given the government-wide authority and responsibility for ADP security. At the same time, its members believed that they needed to be involved in some way. The NCSC's predecessor organization, the United States Communications Security Board (USCSB), had studied the problem earlier and had "concluded that a void existed which the USCSB, now the NCSC, could fill."⁶ The NCSC decided to look at the problem once again. In January 1980 the chairman of the NCSC appointed a Computer Security Working Group. The working group was asked first to "examine those aspects of computer security that relate to teleprocessing systems," and then to "develop objectives, policies and implementation procedures for consideration by the NCSC."⁷

To perform these tasks the working group established three subgroups, the first to survey present government computer security policy, the second to examine operational requirements and problems, and the third to analyze the results of the first two and to recommend any necessary changes or additions to existing policy.⁸

The final report of the Working Group did an excellent job of detailing the muddled state of information security policy. It made note of "the number of existing bodies involved in information systems security" and reported that the Policy Survey Subgroup "found fragmentation of policies and responsibilities and lack of cost effective, feasible implementing guidance."⁹ But the report did little to untangle the muddle. In fact, it may have exacerbated the situation by reaching apparently contradictory conclusions. The report seems to say that additional policy is needed while, at the same time, stating that additional policy is unlikely to be beneficial and may even be counterproductive.

In making the case for more policy the report states, "There is a need for additional policy guidance on computer systems security . . . for the protection of all types of sensitive information in telecommunications systems and computer networks." It notes that some of the existing policy limits itself to "ADP systems security" and fails to deal explicitly with "data in telecommunications systems or computer networks where the needs for systems security in the future appear to be greatest." The report ultimately calls for a "national level group" to review the situation and to recommend a coordinated "National level approach" to information system security policy.¹⁰ Taking note of the civil-national security split, the report states:

Promulgation by a National Authority should proceed under conditions in which participation by both the national security community and non-national security communities is assured to recognize the requirement to protect all types of sensitive information.

On the other hand, the Working Group also concluded that:

[T]he amount and nature of existing computer security policies on one hand, and the results of various . . .

oversight activities on the other, suggest that the root problems of computer security program implementation in the field are not going to be substantially ameliorated by simple promulgation of additional overall policy.

Moreover, the comprehensive nature and recency of the promulgated OMB computer security policy requirements suggests that issuance of additional overall computer security policy per se from a different and potentially competing "national"¹² level source may, in fact, be counterproductive.

The report cites as possible effects of additional policy further confusion, a duplication of effort, conflicting guidance, dissipation of already scarce resources and expertise, and even possible government embarrassment.¹³

The report goes further and questions the utility of policy alone. Noting that "a large part of the problem is technical in nature and not a policy issue,"¹⁴ the report states:

In some cases, organizations are charged with a responsibility ("secure their computers") with varying degrees of a clear definition of what that means, how to do it, or how to prove they have succeeded.¹⁵

The Working Group clearly recognized the importance of the development of technical expertise.

The apparent contradiction in the recommendations of the Working Group may be due in part to an inherent conflict between competing objectives. In technical fields, particularly, there is a constant pressure to distribute functions and divide responsibilities in order to secure the principal advantage of specialization -- the development and maintenance of competence and expertise. Yet this pressure runs headlong towards and eventually collides with an equally strong desire for the improved managerial effectiveness that can only result from uniform policies and centralized control.

The muddle, then, seems to be partly a direct result of the unending tug-of-war between the pro-centralization and pro-decentralization stances. The adequate addressing of some of the technical problems noted by the Working Group may require the single-minded pursuit of an elusive goal. This, in turn, may almost demand continued separation -- as long as the problems themselves are separable (see succeeding chapters). But a complete solution to the policy problem likely requires a single authority, as the report of the Working Group suggests and as NSDD-145 is now attempting to provide. Thus, the Working Group consciously or unconsciously seemed to be searching for a balance, while simultaneously recognizing the inherent difficulty.

The Paperwork Reduction Act of 1980 can also be seen as an attempt to deal with some of the policy muddle. As contrasted to the NCSC's effort, the act concentrated more on the government's civil sector. By establishing a governmental focus and by setting forth specific responsibilities, the act could have advanced the state of information security within the federal government -- particularly its civil agencies.

According to the GAO, this has not happened. For its failure to do so, the GAO blames both the central agencies (OMB, DoC, GSA, and the OPM) as well as the individual executive agencies. The GAO's findings were that:

- OMB Circular A-71, Transmittal Memorandum No. 1, is not sufficiently comprehensive to provide needed policy and guidance to executive agencies for establishing a reasonable level of protection over their automated information systems. . . .

- The central agencies have not been effective in fulfilling their automated information security program responsibilities. . . .
- Executive agencies are doing little to implement information security program policy and guidance. . . .
- Executive agencies have not developed and maintained a total system of controls to eliminate the fraudulent, wasteful, abusive, and illegal practices to which their automated information systems have been and are being subjected.

As was pointed out in the previous chapter, the GAO may be reading more information security into the act than Congress had intended. The act certainly appears to take a significant step toward eliminating some of the computer-communications split by assigning both "automatic data processing" and "telecommunications" functions to the Director of the OMB.¹⁷ What is not clear, however, is that the move toward centralization was ever intended or is being interpreted -- by other than the GAO, that is -- as extending to security issues. Since both the act's legislative history and its accompanying report are mute on the subject, no clues to Congress' original intent are available.

The GAO apparently does see the Paperwork Reduction Act as a deliberate instrument of information security and thus its report is quite critical of what the GAO perceives as an unenthusiastic response to the act on the part of executive agencies. The report is especially critical of the OMB, stating:

OMB has not effectively assumed its leadership role as set forth in the Paperwork Reduction Act of 1980, particularly that portion applicable to information security programs.

Specifically, the GAO report blames the OMB for not making its Circular A-71, Transmittal Memorandum No. 1 "sufficiently

comprehensive to provide needed policy and guidance to executive agencies for establishing a reasonable level of protection over their automated information systems."¹⁹ According to the GAO report:

. . . the memorandum does not (1) identify the minimum controls necessary for ensuring a reasonable level of protection over personal, proprietary, and other sensitive information, (2) clarify the relationship between Transmittal Memorandum No. 1 and policy and guidance on safeguarding information classified for purposes of national security, (3) clarify when executive agencies must afford the same level of protection against unauthorized disclosure of personal, proprietary, and other sensitive information as they do to information classified for purposes of national security, and (4) establish a policy and specific guidance for achieving a reasonable level of protection over those systems using telecommunication networks.²⁰

It is perhaps worth noting that the first three of these problems result from the civil-national security split and the fourth is a reflection of the computer security-communications security separation.

In its report the GAO asserts that some, but not all, of what it terms "personal, proprietary, and other sensitive information" needs an amount of protection equivalent to that given classified information and it faults the OMB for not specifying which part. The report notes that, within the intelligence community, the common tendency is to afford this "sensitive" information the same protection as that which is classified.²¹ This is probably due less to some philosophical conviction regarding the amount of protection required than to the expense and technical difficulty that would attend any attempt to handle the two kinds of information differently.

The GAO report also cites the OMB for not making any real efforts at enforcement:

Our current evaluation shows that other than issuing circulars, OMB has not taken any further action to ensure

the executive agencies' effective implementation of their information security plans.²²

But, this enforcement problem goes beyond the OMB. If the OMB has been guilty, as it surely has, of placing too much store in unenforceable regulations, what about the Congress itself? The act appears to leave Congress equally impotent. Here we have a case where Congress passes a law that "requires" a federal agency to do something. The agency fails to do it at all, or at least fails in the eyes of the GAO, Congress' watchdog. The GAO investigates and advises Congress that the agency is not doing what it was charged to do. These are precisely the circumstances surrounding the Paperwork Reduction Act. The question is, "Now, what?" What can Congress do? Presumably, it can be a bit more tightfisted with that agency's budget in the future. But this game is a hard one to play. Congress is made up of 535 individual members, each with his or her own political agenda. More often than not, some other item on this agenda intrudes and dominates whenever budgets are considered. Theoretically, the law could be enforced through legal action, but it is not clear who would bring suit. Absent effective enforcement of its information security provisions, the Paperwork Reduction Act has not proven particularly influential.

Part of the problem with the Paperwork Reduction Act is that it seems to be gripped by the power-restraint dilemma described in Chapter 1. The act charges the director of OMB with "providing agencies with advice and guidance about information security." Yet it also charges the director with "promoting . . . greater sharing of information by agencies."²³ As Chapter 1 pointed out, these goals

tend to be in conflict and the best the OMB director may be able to do is to seek some reasonable balance between them.

Both attempts at dealing with the policy muddle -- the NCSC Working Group for the national security sector and the Paperwork Reduction Act for the civil sector -- shared a common thrust. Although the NCSC report itself questioned the utility of such an approach, both attempted to deal with the problem by assigning responsibility. They both appear to reflect the belief -- or at least, the hope -- that the government's information security problem can be solved if everyone knows who is responsible for what. What they demonstrate, instead, is that it is far easier to pass laws, to promulgate policy, and to issue regulations than it is to grapple with the thorny issue of balance or to achieve real technical progress.

The lesson from both seems to be that information security will not result from policy or administrative procedure alone. To be helpful, policy must be supported by technology. As one government official expressed it:

. . . I will sum up what we on the policy-oriented side of the picture perceive: the primary barrier to both more valid and responsive policy per se, and more importantly, to cost-effective implementation of that policy in the field, remains the relative status of the hardware/software security subdiscipline -- the lack of relatively secure system foundations in the first place and the associated lack of standards, criteria and guidelines for both how to get there and how to determine when you have arrived.²⁴

Yet, at the same time, technology constraints cannot be permitted to dictate policy. This may be precisely what has happened within the DoD. As NSA Director Lt. Gen. Lincoln D. Faurer has stated:

I must confess that an informed view is that the creation of policy and regulation on this issue have, in a sense, been geared to the technology available to support it.²⁵

There has been a noticeable tendency on the part of the DoD to avoid setting any policy that implied a requirement for something it perceived it could not obtain.

Thus, the evidence suggests that the DoD has deliberately kept the policy weak to remain within the levels of protection that technology could already supply, whereas the civil side seems to have totally ignored practical considerations. If policy demands no more than what is already achievable, there is little incentive for investing in additional research and development. On the other hand, if regulations are framed in total ignorance of what is technically possible or feasible, they run a strong risk of being ignored. Neither side appears to have found that preferable middle ground where policy establishes a standard somewhat beyond the reach of current technology but permits temporary deviance from this standard so long as the deviance is for a specific stated time and is accompanied by a commitment, backed up with funding, to attain the prescribed standard within that time.

Perhaps, with the new policy framework offered by NSDD-145, this middle ground can be found. The new directive certainly seems to untangle the policy muddle. It establishes the National Telecommunications and Information Systems Security Committee, which operates under a cabinet-level steering group and is charged, among other things, with developing and promulgating national policy for both communications and computer protection. And, since NSDD-145 allows a somewhat broader interpretation of national security information and makes no mention of non-national security related

information, it avoids the definitional problem that plagued the implementation of PD-24.

But it is not just policy that has been in a muddled state. Although, as Figure 1 shows, policy responsibility has been the most diffused, other functions are distributed as well, according to the national security-civil and the communications-computer split.

FUNCTION	NATIONAL SECURITY		CIVIL	
	Communications	Computers	Communications	Computers
Policy	NCSC	ODUSD (Policy) /DCI	Subcommittee on Telecommunications Protection	OMB
Standards	NSA	NSA	NBS/NSA	NBS
R & D	NSA	NSA, Services, Agencies, & Industry	Industry	Industry
Production	NSA	Industry	Industry	Industry
Procurement monitoring	NSA	OSD(COMP)	?	GSA
Evaluation	NSA	NSA for products; Services & Agencies for applications	NSA	Agencies
Personnel security	Services & Agencies	Services & Agencies	Agencies	OPM
Technical advice	NSA	NSA	NSA/NBS	NBS

Distribution of Security Functions Before NSDD-145
Figure 1

In some cases the actual dispersion is not quite as stark as the chart implies. The chart depicts official responsibilities, but not the sharing of tasks, which takes place unofficially. While perhaps quite helpful in overcoming some of the disadvantages of decentralization, this interaction is not in accord with official charters or even the official "party line" of the organizations involved. Thus, some of the task sharing that has actually been going on may not even be admitted. For example, on the civil side, in the area of computer security evaluation, the chart shows that individual agencies are responsible. Yet, according to the personal observations of a government official:

There are agencies that work with the Department of Defense agencies -- civil agencies working with Department of Defense on their independent evaluations. So, even though, officially, some civil agencies say, "We're very reluctant to work with anybody in the DoD," unofficially, there's quite a working relationship.

Presumably, task sharing will increase as the new directive is implemented. For the present, however, the chart's general picture of widely distributed responsibilities remains accurate.

All of this arbitrary and artificial divvying up the pie -- no matter how unavoidable -- has served only to confuse and diffuse, ultimately contributing to the present muddle that NSDD-145 addresses. So long as the muddle is allowed to persist, in the opinion of many, there will remain an abundance of inadequately protected systems. The General Accounting Office is blunt in its judgment: ". . . executive agencies' automated information systems and the assets they control are exceedingly vulnerable to misuse, abuse, and theft."²⁷

This judgment is made in spite of efforts to ameliorate the situation. In computer security, as Chapter 6 has shown, there have

been attempts at legislative and administrative "fixes" as well as technical ones. However, these remedies do not appear to be working and the technical fixes are not proceeding very quickly. The result is very little progress toward the goal of protected systems.

According to one writer:

Despite a growing awareness of computer vulnerability, the current status of computer security in most installations, when compared to the current level of technical sophistication, can most charitably be described as primitive. We have figured out how to make computers faster, smaller, and more efficient, but computer security, by and large, is still at the "lock on the door" stage. . . .

The assessment, then, of the current status of computer security is that the culprits are riding in automobiles while the cops are still on horseback.

Robert Ellis Smith states in Datamation that, in spite of precautions, ". . . systems remain incredibly vulnerable to those who would rip off assets or alter data." The problem does not seem to be due to any lack of awareness, for, as Smith points out:

At a meeting sponsored by the Department of Commerce in May [1982], representatives of major banks, businesses, and government agencies simply admitted that their systems were not protected against unauthorized access.

In fact, there is very little argument over either the vulnerability or the rather primitive nature of present security mechanisms. Regarding the availability of mechanisms, Edwin L. Jacks, then with General Motors' Information Systems and Communications Activity, has stated:

Commercially available computer systems today only in part support the building of secure information systems. The security objective of maintaining availability, integrity, and confidentiality under adverse conditions are not inherent in most commercial systems

Although Jacks' statement was made in early 1980, the situation has not changed much as of early 1985.

There is considerable argument, however, over whether or not the vulnerability constitutes either a serious or a solvable problem. A June 1982 article in the IEEE Spectrum contained this appraisal:

Despite such vulnerability, opinion is divided on whether computer security is a serious problem. Some experts contend that adequate security can never be attained, either because it would cost too much or the increased restrictions would result in unbearable losses in system performance or in user freedom to communicate. . . . Other experts say that the technology already exists to make ³¹fail-safe security systems for at least current applications.

The February 1983 issue of Datamation included a transcription of a panel discussion arranged by the Computer Security Institute at its 1982 annual conference. Among the participants were Robert H. Courtney, president of a New York consulting firm, Peter S. Browne, vice president of Burns International Security Services, and Warren Schmitt, senior project manager of data security for Allstate Insurance. They were discussing the present state of computer security, particularly within the business sector. Their comments reveal serious disagreements.

Courtney maintains that the problem is not out of control. "We are not falling behind,"³² he is quoted as saying. Courtney also believes that any shortcomings in data security have not placed organizations in great jeopardy.

Schmitt and Browne, on the other hand, both believe that we are behind. Browne goes even further when he claims that "we are continuing to fall behind" because "the increases in speed, complexity, proliferation and use have outstripped management's ability to control." It is Browne's contention that the degree of risk faced by most organizations is not at an acceptable level. He concedes, however, that "we are struggling to reach that level."³³

The problem seems to be more one of motivation than of technology. As Courtney puts it, "We don't lack the technology or the smarts, although I think we have a shortage of motivation." And Schmitt adds that "in areas that are experiencing the greatest change, such as access controls and networking, the control issues are not so well understood" which, he says, "makes it difficult for both management and technicians to support effective security efforts."³⁴

At another panel session on computer security, Leslie S. Chalmers, an Assistant Vice President of the Bank of California, remarked, "There are many companies out there who have no security program whatsoever." She then told of being at a recent conference and meeting an EDP auditor from a "rather good-sized conglomerate." He told her that one of his company's subsidiaries was in the business of producing pharmaceuticals -- including controlled substances. This subsidiary had, according to Chalmers' account:

. . . developed a system in which they allowed their customers -- pharmacies -- to dial into their computer and order drugs Not only did they allow this, they allowed their customers to change their own names and addresses.

She then remarked, with appropriate incredulity, "They don't think they have a security problem!"³⁵

The above-quoted persons were speaking primarily of computer security in the private sector. However, turning to the federal government the situation is little different.

Examples abound, but perhaps the most notorious (and oft-cited) is that of the Social Security Administration (SSA), an agency of the Department of Health and Human Services (HHS). The SSA administers a number of social insurance and welfare programs. A September 1982

report of the House Committee on Government Operations depicted the SSA computer system as having "no adequate controls to prevent fraud and abuse" and as "essentially wide open to potential theft."³⁶ The report blamed much of the problem on "the apparent indifference by top agency officials" and refers to 34 reports since 1974 by the GAO alone that describe a computer management problem at the SSA and that collectively contain 90 recommendations, most of which, according to the committee report, "SSA has effectively ignored."³⁷ The report attributes "billions of dollars of erroneous payments" to SSA's mismanagement and points out that when confronted with evidence of possible fraud (such as one person accepting benefits in the name of someone else), ". . . SSA always presumes that an error had occurred. There is no effort to detect or deter this kind of fraud."³⁸ The report concludes with the following statement:

When asked directly, the SSA personnel confirmed that there were no personnel assigned to deter or to detect employee fraud and that no anti-fraud³⁹ measures were in effect. They knew of none being planned.

An earlier internal HHS report, prepared by the department's inspector general's office, serves only to reinforce the committee's observations. According to the November 1981 report, SSA computers are so poorly protected that sensitive, private information or benefit payments could easily be obtained by unauthorized people. The report stated that computer terminals at the central office in Baltimore are easily accessible to unauthorized people and often are left unlocked and unattended, and that "weakness in access controls subjects sensitive, private information on SSA files, including benefit payment data, to unauthorized use and manipulation." Comparing the 1981 situation to that in 1977 when an earlier study was made, the 1981

report concluded that the state of COMPUSEC had deteriorated rather than improved and specifically noted that the number of poorly protected computer stations in the Baltimore headquarters rose from 48% of the total in 1977 to 60% in 1981. Perhaps the most troubling deficiency concerned the use of personal identification numbers. These numbers are assigned to employees authorized to process disability cases when quick payments are required. The report pointed out that unauthorized persons could gain access to these numbers, making it very difficult to trace who had approved the payments.⁴⁰

Admittedly, determining how much security a system should have is a matter of balancing cost against risk, but the record suggests that the SSA made no attempt to do so. The earlier cited House Committee report concluded that:

Agency officials have made little or no effort to implement even the most fundamental security measures that would protect its valuable resources from the theft, misuse or catastrophe.⁴¹

According to a 1983 article in the U.S. News & World Report, this problem is now being addressed. The article reports that the SSA "is spending 500 million dollars to modernize its computer and make them more secure." "But", the article adds, "it will take five years to put the new system in place."⁴²

Although the earlier situation at the SSA may have been extreme and not representative of the general state of information security among civil agencies, neither is that state what many believe it should be. In the words of James H. Burrows, Director of the Institute for Computer Sciences and Technology at the NBS:

I really don't see the civil agencies paying a hell of a lot of attention to it [technical computer security] . . . [T]hey quickly run across the fact that they've got a personnel problem they've got to get by first.⁴³

According to Burrows, civil service regulations "stand in the way." Burrows is referring to those regulations that seek to provide the career civil servant with a measure of job security and thus to protect him from adverse actions on the part of his politically appointed bosses by imposing strict procedures for all adverse actions and providing for an appeal process. The practical effect is to make it rather difficult to remove a federal employee, even for cause. Burrows goes further than most critics of the regulations and offers a case for taking action "on suspicion." As he points out:

. . . if you can't remove people from sensitive positions on suspicion, that means that you have to be burnt before you can take any action. Then, in fact, you have to prove the guy not only burnt you but did it maliciously or intentionally

According to Burrows, it is even difficult to place an employee in a less sensitive position. He says:

In almost all places in the government, all personnel actions are subject to review. A guy could petition and say he wasn't treated correctly. So it's very difficult.⁴⁴

To illustrate his point, Burrows relates a personal incident that occurred when he worked within the DoD:

I had a guy in the basement of the Pentagon who started a fire in the computer room. We fired him on the spot [A] year and a half later, he came back, he got full back pay, promoted one rung and [they] told me we had to find him a job.⁴⁵

The reasons for the present state of inadequacy within the civil sector are many and varied. They certainly include unawareness, indifference, and ineptitude. For example, when Burrows was asked for his reaction to the Walker proposal for the establishment of a Federal Computer Security Evaluation Center at NBS,⁴⁶ he replied:

My reaction was: It would be a useful thing; we could probably do it, but, in one sense, the civilian part of the government is not ready for that⁴⁷

GAO's Podell attributes the unreadiness to indifference, saying, "What I would expect from the civil agencies is a definite interest in meeting our recommendations for improved security -- a commitment." But, he acknowledges sadly, "They're not all overwhelmingly enthusiastic."⁴⁸

There is also the matter of priority. According to Burrows:

It's not a technical problem. They haven't closed the first barn doors. Why worry about the third level and fourth level barn doors when they can't even protect themselves against their people.

Burrows went on to cite the absence of risk analysis as a further problem within civil agencies.⁴⁹

The earlier cited GAO report had also commented on the absence of risk analysis. "During our evaluation," said the GAO study, "we did not find any executive agency performing a comprehensive risk analysis"⁵⁰ This, despite the fact that OMB Circular A-71 specifically requires it. The GAO report goes on to state:

Without performing a risk analysis, which is an essential first step in developing an information security program, many Federal agencies' information security programs remain unnecessarily vulnerable to accidental abuse and deliberate acts of sabotage, fraud, waste, and other forms of inefficiency.⁵¹

The report continues:

Since risk analysis techniques are not generally used in executive agencies, senior management is unaware of how vulnerable their information systems really are to unauthorized and illegal problems.⁵²

GAO describes the information security problem as "highly complex and technical." Asserting that senior managers have been successfully shielded from the problem, the report states that "they have seen little reason to provide the needed financial and budgetary support to develop and maintain a reasonable level of protection"⁵³ In

fact, the GAO report implies that the problem is circular because, lacking specific vulnerability data, "senior management has been reluctant to allocate sufficient time and resources . . . to perform the needed internal review function."⁵⁴ Thus, without a review or audit, no specific vulnerability data is obtained, and absent specific vulnerability data, there is no internal review.

A widespread reluctance or an inability to think in terms of long-term solutions is also evident. Dr. Peter G. Neumann of SRI International recalls serving on a panel of the National Academy of Sciences that was looking into computer security needs of the federal government. Neumann relates:

Many of our briefers would not admit that they had a problem. You ask them what are their requirements for the future and they very diligently describe their requirements of today, because they're afraid if they describe something they can't have, they will get shot down or they will not be able to obtain it because the risk is too great, or whatever. I'm not quite sure what the motivation is, but we got this over and over again. We got stonewalled by people who would, essentially, think only of their very limited problems of today.⁵⁵

Yet, all admit that any "solution" to the information security problem will only be found in the long term. It will certainly not be found soon.

Nor has the Department of Defense solved its computer security problem. In a September 1981 speech to the IEEE Computer Conference, NSA Director Faurer made this point explicitly when he stated:

The majority of computer systems in use simply do not have security of data as their primary objective. Users are most interested in performance, reliability, ease of use, and accountability -- as they should be. Contemporary computer systems simply do not provide reliable protection of their data, and contemporary systems are often distributed, with security problems compounded by remoted terminal or network considerations. . . .

Management awareness of the problem across the Department of Defense needs considerable bolstering. This is not an easy matter! Computer Security aspects of computer operations are viewed by most as a black art, and most officials can hardly be blamed for simply settling for assurances that they ⁵⁶are in compliance with computer security regulations.

Within the defense sector, in spite of statements by Faurer that ". . . the concern within Defense about computer security is a very genuine one,"⁵⁷ there are those who question the level of the department's commitment. One such person is Roger R. Schell, formerly an Air Force Colonel assigned to the NSA:

I claim that we today have the ability to have a significant improvement in the security of 80 percent of the processing which is done in the Department of Defense. We have the technical ability. We've had it for four to five years. We are not doing it. We don't have the will . . . because it costs money.

Schell's estimate to accomplish this "significant improvement" is a 10% increase in cost, which, as he is quick to point out, "is a big number." Although he believes that it would be worth the 10%, he says that decision makers "don't want to hear it" because a significant portion of it would involve "up-front investment and what they don't want to hear is the bow wave."⁵⁸

MITRE's John P. L. Woodward also questions the DoD's commitment to computer security. His doubts arise from the looseness of the present regulations and the relative ease with which they are either waived or determined not to apply.⁵⁹

And James Anderson, a long-time computer security specialist, adds:

If the government really believed that this was important . . . they would modify procurement regulations; . . . they would install procurement regulations and make them work; they would dramatically disqualify some popular vendor on some procurement on the basis that they didn't

meet some security standards; and [they would] reward those who have done the work on it [computer security]. If no one qualified, reward those that come closest.

Anderson adds ruefully, "I know that's an unrealistic hope."⁶⁰

Anderson compares the commitment to COMPUSEC with that to COMSEC when he states:

The degree of seriousness that has been represented in the crypto game has not existed in the computer security game. . . . We've been at the [COMPUSEC] game . . . 15 years, and we're still fooling around the edges.

When asked why Anderson thought this difference existed, he replied:

I really don't know. I think it's a matter of perception. I think people understand the reason for secure communications because of history [P]eople understand the danger of not having secure communications.⁶¹

(Although people may understand the need to secure their communications, many still fail to do so. The point of Anderson's statement is that the situation on the COMPUSEC side is even worse.)

Woodward offers another reason for the difference in commitment levels:

The reason it [COMPUSEC] is not taken seriously enough is because the answers are not as known as in the COMSEC world and the costs are very prohibitive. The costs of providing security in a verified sense are very high.

Woodward also points out that the DoD program manager's emphasis is most likely to be aimed at simply getting his system approved ("accredited" is the official term). He is not likely to invest any more on security than he has to in order to obtain this accreditation.⁶²

According to Woodward, industry has learned to gauge the level of the government's commitment:

I've talked to contractors about this, and their view of it is, "So, we get in an RFP [Request for Proposal] and the RFP has a whole bunch of security requirements in it, but

they're in there with a whole bunch of other requirements that are conflicting -- like you have to have high performance; you have to have this and that." There's no awareness in the RFP that these things trade off against each other. The contractor has to decide -- without knowing how his proposal is going to be judged, without knowing the weights of the various portions -- he's got to decide how to bid it. Historical precedent says, "Don't pay too much attention to the security if it trades against anything else," because that's how contracts have been awarded in the past. So the contractors really don't know how seriously to take the security requirements and they usually end up either downplaying them or ignoring them or just paying them lip service and not really considering them. And, they get away with it!

Even when the government tries to require security features, it is sometimes thwarted by outside pressure. Schell offers the Air Force experience with SACDIN (originally called SATIN IV) as an illustration. (The following account is based upon information supplied by Schell, but its major elements have been corroborated through three other sources.)

Common practice within the DoD, particularly on a large or sophisticated procurement, is to distribute draft copies of the Request for Proposals (RFP) in advance of the official issuance of the RFP. This is often done even before the government has the money available that would legally permit it to solicit. For example, the pre-solicitation, as it is often called, might be done late in the fiscal year prior to the one in which the program has been budgeted. This accelerates the process by shortening the time allowed for the official response; it can provide the government with very useful feedback; it can alert the government to situations in which the RFP might not generate enough bids to make the solicitation sufficiently competitive; and it gives a particular company a chance to prepare itself -- to assemble a team of people who will be ready to begin a contractual action should the company win the award.

In its draft RFP for SATIN IV, the Air Force specified a requirement for a security kernel as the basis for security. Schell recalls that "this was probably near the high point of the computer security influence on industry." According to Schell, the RFP generated quite a bit of excitement throughout the industry. "We probably had half a dozen major organizations in industry that were gearing up, hiring people . . .," says Schell. At that time "it looked [to industry] like that was the direction the government was going." "With that sort of momentum . . .," recounts Schell, "the RFP for SACDIN went out to the industry." Then things began to go sour. Schell recalls receiving reports from both government and industry that IBM had contacted an Air Force Assistant Secretary. In Schell's words:

The Assistant Secretary of the Air Force for R&D was approached by IBM and the thrust of what they said was, "Do you realize that you've been suckered and done in, because you're going to kill the whole SACDIN program by requiring that stupid, idiotic security kernel stuff and the program is just going to die. It's not feasible. It's outside what anybody's able to do. You know, you're just going to sacrifice the whole program because of some R&D wienies sitting at ESD. You know, you'd better get your house together."⁶⁴

The Assistant Secretary, Robert H. Scherer, promptly directed that all references to a security kernel be removed from the RFP.⁶⁵ The Air Force's program management team at ESD, like bureaucrats everywhere when they receive direction they do not like, found a way to carry out the letter of the direction but not its spirit. Says Schell:

We had the specifications on line. We did a global substitute with an editor that said, "Whenever it says 'security kernel,' we will say 'internal access control mechanism (IACM)'" . . . and we really made no other changes in that area.⁶⁶

Meanwhile, during the time that elapsed between the issuance of the draft RFP that had called for a "kernel" and the final RFP calling for an "IACM," word of Assistant Secretary Scherer's decision had reached the prospective bidders. Thus, the RFP took them by surprise. Schell reports:

Within two hours of the time of the release of the RFP, I had a number of phone calls that said, "You know, you guys sandbagged us. We killed the security kernel. We got rid of all that stuff. We can't recover it. There's nothing we can do about it. . . . But . . . it's there. You called it something [else], but it's there."

Realizing that industry had been misled, the Air Force people decided that they could no longer make the award contingent upon the incorporation of a kernel. Therefore, in spite of objections from SAC, who still wanted the high degree of protection afforded by a kernel, ESD lowered the relative weight of the kernel in the bid review process.⁶⁷ But the story was to contain one more ironic twist.

It turned out that one of the bidding teams proposed a kernel anyway -- the team consisting of IBM and ITT. Schell recalls that "they put together a very credible proposal for an IACM that was, in fact, a security kernel. They, ultimately, won the bid." When asked if he thought IBM had been trying all along to make it easier for itself, Schell replied:

No. I'm relatively persuaded . . . that they were surprised by the RFP. Everybody was surprised, including IBM. They⁶⁸ really believed that Scherer had gotten rid of the kernel.

As Schell points out, Scherer, himself, believed he had gotten rid of the kernel. Thus, Schell believes that there was no opportunity for collusion. He attributes IBM's success to the fact that, being a large company with a wealth of technical talent, it was simply able to react more quickly than the other companies.⁶⁹ As might be

expected, the entire episode did little to foster a spirit of government-industry cooperation.

In this case, the government was lucky. It ended up with more in the way of security than it had any reason to expect. After all, IBM and ITT had won the contract on the basis of considerations other than security. Woodward says that he believes that, sooner or later, some company will lose a major contract for having downplayed the security requirements. He notes, however, that it has not happened yet.⁷⁰

Facing mixed signals from the government, industry's efforts have been less than all-out. Referring to an increasing demand for computer security mechanisms, the director of the DoD's Computer Security Evaluation Center told an industry audience:

Industry's response to this burgeoning demand for automated information services on a worldwide basis has, for the most part, sidestepped the issue of information protection. . . . [A]n ADP industry hard pressed to meet the current demands has found little time or much enthusiasm for providing "secure" or "securable" products.

According to Faurer, this is not likely to soon change. In his IEEE speech he stated:

Despite the progress that has been made, there is a major shortage of good computer security technology. Industry leaders have told us that this situation will continue, in the absence of a certain commercial market willing to pay for such products. We also observe that such technology as does exist does not enjoy widespread use. There are many reasons for this; ignorance of the attributes of the product, performance degradation that is unacceptable, or cost.⁷²

Still, there are some encouraging signs. One factor that has inhibited industry's unqualified commitment to trusted product development is the lack of any government criteria by which such products could be judged. Shortly after its establishment, the Computer Security Evaluation Center at NSA began work on such

criteria. The first draft of the criteria was unveiled on 24 May 1982 at the Fifth Seminar on the Computer Security Initiative.⁷³ The draft invited comments and criticism. These were considered in a later draft and in the final version, which was issued on 15 August 1983. The Preface specifies that the document is intended to serve three objectives: to help users assess products, to serve as a guide for the producer industry, and to help in system procurement specifications.⁷⁴

The criteria establish four major divisions of security protection ranging from Division D, the weakest, to Division A, the strongest. Within each division except Division D, the criteria establish numerically-designated classes in which higher numbers denote stronger systems. In all, eight division-class categories are defined. In order of increasing strength, they are: D, C1, C2, B1, B2, B3, A1, and "Beyond A1". Each successively higher class includes all of the security features of the classes below it and some additional ones as well. Security features appear in six requirement categories: policy, marking, identification, accountability, assurance, and continuous protection. For each category and each strength class, a minimum set of specific features is described. In order to earn a particular class rating, a given product must include all of the specific features for that class in all six requirement categories.⁷⁵

Although the various classes are intended for different applications requiring different degrees of security protection, some people in industry are concerned that the hierarchical arrangement

tends to convey the impression that the lower level products are somehow unworthy. Harry B. DeMaio of IBM states:

In the mind's eye of the vast majority of the outside world, A is better than B, which is better than C, which is better than D. Somehow or another, there is an implication . . . inside IBM that all of our products should be A's. A is a different animal than a B, and B's are different animals than C's. Strategically, they have different objectives [T]he definitions, which tend to imply that on the road to security . . . there is a progression from one level to another, is bothersome.

And he points out "there is a marketplace which will always use [a] C."⁷⁶

In spite of such misgivings, the criteria have had an impact. In his keynote address to the Fifth Seminar on the Computer Security Initiative, NSA Director Faurer noted:

For each and every level considered to be within the current state of the art, industry has produced at least one serious candidate. Furthermore, several of these are being pursued as standard products.

Since, according to the criteria, anything beyond Class A1 is acknowledged to be beyond the present state of the art,⁷⁸ the highest class for which there is a competing product is A1. And the COMPUSEC product that appears closest to obtaining an A1 rating from the Computer Security Evaluation Center is the Honeywell Secure Communications Processor (SCOMP). Originally intended as a secure front-end processor, the SCOMP gradually evolved into a multipurpose computer system. It combines what Honeywell calls a "Security Protection Module" with a Honeywell Level 6 minicomputer. By assigning many security functions to the hardware, Honeywell claims to have avoided the system performance penalties encountered by earlier prototype systems that had attempted to do the bulk of the security job in software alone. To make these prototype systems as transparent

to the user as possible, they generally included a software emulator of some operating system that ran on the top of the security kind. These emulators caused most of the penalty in performance.⁷⁹ SCOMP includes no such emulator and thus avoids this source of performance loss. However, it is also not as versatile a machine.

Early indications are that Honeywell may have a winner. An April 1983 Product Evaluation Bulletin from the DoD's Computer Security Evaluation Center at NSA stated:

[A]lthough the formal evaluation is still in progress, it is clear at this point that the Honeywell SCOMP can provide a state-of-the-art⁸⁰ base for a variety of security sensitive applications.

However, as 1984 ended the DoD Center had still not announced the results of its evaluation.

Another encouraging sign is that several civil agencies have begun their own process of security evaluation and certification. Many different methods have been initiated by various agencies including the use of contractors, consultants, and in-house experts.⁸¹ And some, as has been noted, have even gotten help from the DoD.⁸² Meanwhile, the NBS has been developing a set of formal guidelines to assist government agencies in the process.⁸³

The problem with these encouraging signs is time. They are all coming very slowly -- so slowly, in fact, that some people have begun to question the wisdom of the government's strategy, particularly that for computer security, and have begun to ask if perhaps the distributed responsibility is not partly responsible for the slow pace.

Chapter 8

Two Opposing Views

The preceding chapter has shown that, although there are some hopeful signs and trends, the present state of information security in government as well as in business is poor. Among the sources of the difficulty are that responsibility is diffused, authority is sharply limited, commitment often seems half-hearted, vision is frequently short-ranged, and supporting technology has not been readily available. Many people presumably in a position to do something about the problem apparently fail to recognize it at all or, if they do recognize it, hesitate to take action. Yet, there are many other persons who are well aware of the problem and are seriously attempting to do something about it. The question is, "What?" There is evidence of an extreme divergence of opinion regarding the best strategy to be pursued. There are two principal schools of thought. One school holds that there are sufficient differences between COMSEC and COMPUSEC to justify pursuing them separately and even by different strategies. The other believes that trying to maintain the current separation is both artificial and risky.

There are really two concerns here -- that of separateness and that of difference. Although eliminating the separation between COMSEC and COMPUSEC and pursuing them as one and the same would automatically eliminate any difference in strategy, the opposite is not necessarily true. It would be possible to maintain the separation yet employ the same strategy.

However, this distinction is more semantic than real. Much of the rationale offered by those advocating a separation between COMSEC and COMPUSEC is so that different strategies can be pursued. Most computer security people seem to view COMSEC strategy as firmly entrenched and probably immutable. Those who wish for something different for COMPUSEC, therefore, argue for a separation. On the other hand, the evidence suggests that most people who believe that COMPUSEC and COMSEC should share the same strategy also argue that the two should be pursued jointly.

For several years the primary strategy for acquiring COMSEC mechanisms has involved government-sponsored, classified contracts with industry to produce classified products of government-owned design. Although, as was discussed in Chapter 5, some commercial products employing the DES have been developed, these devices have been slow to gain a foothold, and for the more sensitive government situations, probably should not be expected to.

For acquiring COMPUSEC mechanisms, the Computer Security Initiative⁸⁴ constitutes the current major government strategy. The Initiative seeks industry products produced in an open, unclassified environment. From the beginning, the Initiative aimed at the "widespread availability of 'trusted' ADP systems for use within the DoD."⁸⁵ Also from the beginning, it was clearly the belief that "widespread availability implies the use of commercially available . . . systems whenever possible."⁸⁶

The objective, then, has been to stimulate industry to produce these products, based perhaps upon earlier government or academic work, and to support these products as part of their main product lines.⁸⁷

In the words of one consultant, ". . . computer security developments will be meaningless unless they are incorporated in and supported as part of manufacturers' product lines."⁸⁸ And another adds, "The DoD does not want to be in the business of building and maintaining its own line of computers and operating systems."⁸⁹

The alternative to the Initiative's strategy of industry-sponsored development would be for the government to simply decide what it wanted and then pay industry to build it. In this way, the government can ensure that it gets exactly what it wants as opposed to having to accept what industry decides to produce and it does not have to wait until industry perceives a market from within the business sector. As it is, everybody seems to be waiting for everybody else.

However, this alternative strategy presupposes three things:

1. that the government knows what it wants,
2. that it can afford what it wants, and
3. that industry is both willing and able to provide it.

People who oppose this alternative strategy, and therefore support the Computer Security Initiative, can offer arguments against each of these three assumptions.

First of all, they would say that a lack of expertise within the government prevents the government from understanding and thus defining exactly what it needs. Many think that the government lacks the competence in COMPUSEC that it was able to acquire in COMSEC. More than that, many believe that the government could not acquire the needed competence, even if it wanted to. Schell, for example, states, "The government is totally incapable . . . of developing an extensive, independent body of expertise the way they have in COMSEC."⁹⁰

During the 1920s and 1930s the government was able to accumulate the dominant body of knowledge in the COMSEC field. Admittedly, this took time. As Chapter 3 has pointed out, when World War I began the government was forced to seek help from a small privately funded research institute, Riverbank Laboratories.⁹¹ Gradually, however, aided particularly by Riverbank's work in cryptanalysis, the government was able to acquire a position of dominance.

In spite of this success in COMSEC, most observers would argue that the same course is not available to the government in the field of computer security. The first and perhaps the largest problem is that of recruiting. The qualified people the government would need to do the computer security job are exceedingly rare, and therefore come dear.⁹² Because of its fairly rigid salary scales, the government finds it difficult to compete for highly sought talent.

The lack of precise definition adds to industry's risk. Walker addressed this problem in a presentation to the 1980 National Computer Conference when he said:

The DoD and others have been for many years asking the vendors to build trusted operating systems. But since we were unable to clearly define what we mean by a trusted system, industry has been reluctant to undertake a serious development because of the high risk that when completed their product might be found unacceptable by either the DoD or other customers.

Walker went on to suggest a way this problem might be dealt with as a major thrust of the Initiative:

One way to overcome this impasse is for someone (like the DoD) to build a trusted system, demonstrate that it is acceptable in real applications and provide detailed information on the techniques used in the development to the computer industry.⁹³

It had been basically this philosophy that provided much of the justification for some of the kernel development efforts during the mid-to-late 1970s. The report of the Air Force's 1979 Summer Study of Computer Security, for example, stated:

DoD-developed research and development products, such as KSOS and KVM, are necessary to demonstrate that useful secure systems can be built.⁹⁴

The notion was that once the DoD had demonstrated an "existence proof," there would be a deliberate transfer of whatever technology the government had acquired during the development effort. The necessity of such a transfer of technology, according to one report,

. . . can be seen in the fact that even if government specifications were tightened to ask for the kind of security we believe possible with the current state of the art, fewer than fifty people in the country would understand the true implications of what is being asked for, and those fifty are concentrated in less than a half-dozen organizations, none of them in the main stream⁹⁵ development organizations of the major mainframe vendors.

The requisite experience is indeed rare.

Then, there is the matter of cost. Cost has been a major area of concern and a significant factor in shaping the government's computer security strategy. As the report of the 1979 Air Force Summer Study stated:

. . . until the manufacturers offer [secure] systems as widely supported products, we will be unable to have more than a few prototype applications because of the high cost of development and support.⁹⁶

In 1972, the Computer Security Technology Planning Study, commissioned by the Air Force and chaired by James P. Anderson, determined that to start over and redesign an existing system essentially from scratch "is likely to exceed \$10 million dollars per system type."⁹⁷ And this was in 1972, when dollars bought more and

extant systems were simpler.

Presently there is no benchmark for projecting the cost of a secure system. Costs will vary widely according to their other-than-security functionality and according to the degree of security protection they provide. It now appears that some amount of protection might even come free, as computer vendors evolve security features into their main product lines. But this "free" protection is likely to be classed somewhere in the range of levels between C2 and B2⁹⁸ -- sufficient certainly for many business and DoD "controlled mode" applications but inadequate for most DoD multilevel applications.⁹⁹ Systems sufficiently robust to withstand the full range of threats, which national security applications must be prepared to face, are likely to be very expensive. People in the business hesitate to quote a figure, probably because they do not wish to frighten anyone off. When pressed, however, some will admit that a premium of between one and two orders of magnitude might be required for a multilevel secure system over a non-secure one of comparable functionality -- if such a system could be developed at all.¹⁰⁰ To be judged "multilevel secure" in a general sense, a system would probably have to be capable of coping with five or more security levels. To do so it would have to be able to stand up to subversion (discussed later in this chapter). And to be considered strong enough to withstand subversion, a system would surely require a rating beyond A1. But even the DoD's evaluation criteria document acknowledges that "Most of the security enhancements envisioned for systems that will provide features and assurance in

addition to that already provided by class (A1) systems are beyond current technology."¹⁰¹

Mitigating the DoD's concern for cost, however, has been its conviction that its needs were not unique -- that "the underlying operating system support needs of the DoD are so little different from those of other ADP users that the expense of DoD unique operating systems cannot be justified."¹⁰² In addition, the DoD's belief has always been that it lacked the leverage necessary to persuade industry to build these "trusted systems" unless industry perceived a market outside the DoD as well. It was Assistant Secretary of Defense Dinneen who articulated this point at the first of a series of joint government-industry seminars on the Computer Security Initiative. He said, ". . . before the industry will invest much effort in trusted systems, they must be convinced that such systems are reasonable for use on broader government and private sector sensitive handling applications."¹⁰³ Therefore, the Initiative's thrust has been to convince industry that the DoD needs are not unique and that trusted systems developed for the DoD would find applicability and marketability elsewhere. The success of the government's strategy hinges on the government's ability to convince industry that the risk is, if not minimal, at least acceptable and worth taking.

If the government could thus persuade industry to undertake the development itself, the government would not only save much of the cost of development (less that which is amortized over all units) but it also could expect to pay less per copy because the devices would now be produced in significantly larger quantities, yielding economies of scale.

Finally, opponents of a government-risk strategy argue that the way in which computer companies are organized would impede efforts at providing what the government really wants, which is the best effort of the company's most competent people.

If the government contracts for the development with industry, it is likely to find itself dealing with the part of the company established to handle government business.¹⁰⁴ Although this internal element might be knowledgeable of the government's needs, and certainly with government procedures, it may not be the most competent element from a technical standpoint. For example, if a secure operating system is required, a given company's most competent people are far more likely to be found in the group designing commercial operating systems than in the government products organization.¹⁰⁵ Thus, the government is forced to accept a product from what might be viewed as a second-string organization. For most government needs this is undoubtedly sufficient, but when dealing with something as technically exotic as secure operating systems, anything short of the first string is probably not acceptable. As Woodward has noted, "Developing a good operating system is not a science. It's an art."¹⁰⁶ (Industry's capacity to respond to the government's needs is dealt with further in Chapter 11.)

A second major area of disagreement between the two viewpoints, in addition to that over who pays for the development, is over the matter of secrecy. In a report written by SRI International for the NTIA, the two points of view are very clearly stated:

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.¹⁰⁷

In general, COMSEC people favor the strategy of secrecy while people associated with COMPUSEC favor the strategy of openness. As was pointed out earlier in this chapter, a basic feature of the Computer Security Initiative has involved an open sharing with industry. Although there is precedent for such sharing to take place on a classified basis,¹⁰⁸ the clear intent of the Initiative has been to conduct this sharing at an unclassified level. The Director of NSA himself stated:

We are committed to having the research done and the results disseminated in an open and unclassified manner, except in those exceptional cases where we are working on a previously classified basis.¹⁰⁹

Behind this disagreement over whether a policy of secrecy or openness would best serve U.S. interests are important historical and philosophical differences.

With respect to the historical differences, as was pointed out in Chapter 2, the communications security business proceeds from a tradition of secrecy. There are two reasons for this -- one defensive and one offensive. In the words of one writer:

First, knowledge of the electronics or mathematical coding processes by which the information is scrambled may provide a "leg-up" for potential eavesdroppers dedicated to breaking the codes and reading the communications, thus jeopardizing the protection afforded by one's own protection system. Second, proliferation in the public domain of know-how and/or technology used in protecting communications -- especially in the form of finished equipment -- could enable potentially hostile foreign powers, terrorist groups or criminal elements to protect their own communications and thus deny U.S. intelligence agencies and law enforcement officials a source of valuable information.¹¹⁰

Essentially the same point was made by a former COMSEC practitioner:

Well, the reason that we classified everything in communications security development was sort of two-fold. One is, you have a team of highly specialized analysts look at this and they say, "Yes, it is secure," but someone else may look at it and find a flaw in it. The less that someone outside can find out about the equipment, or its analysis, its operation, the harder job he has to analyze it.

Another reason is that we don't like to have these techniques made available to other parties. Because we think they're good enough for our traffic, he may incorporate them¹¹ in his traffic, and that would cut off some of our sources.

Secrecy in COMSEC has served the country well. Throughout World War II, the U.S. and the United Kingdom routinely broke the machine ciphers of both Germany and Japan. Yet, there is no evidence, even today, that the reverse happened. If either country were routinely reading U.S. or U.K. communications, it almost surely would have discovered the extent to which its own were being read and would have taken action to prevent it. The fact that this did not happen is the best, albeit inconclusive, evidence we have that our communications remained secure. In his book, The American Magic, Ronald Lewin emphasizes this point:

When one considers the colossal volume of radio signals sent out during that war from Bletchley Park, from Arlington Hall, from . . . Washington,¹² or crisscross over the theaters of war, and when one considers that the intercept stations of the Japanese and the Germans must certainly have picked up these myriad transmissions, it seems astonishing that over the years their cryptanalysts -- many of high quality -- never achieved a breakthrough. We must ascribe this not merely to security . . . but also to the high technology of the Allies which produced those enciphering machines -- the Typex, the Sigaba -- to whose protection, as it turned out, millions¹³ of Ultra signals could be entrusted with perfect security.

The computer security field has not shared this secretive history. From the very beginning, most of the significant work in COMPUSEC has been openly published.

One might be tempted to explain this difference by the fact that we were at war during much of the early history of U.S. COMSEC development, but not as COMPUSEC has developed. However, as Chapter 3 has related, most of the significant early developments of COMSEC devices actually took place between the two world wars -- not during them. We must, therefore, seek our explanation elsewhere.

An alternative possibility might be the relative extent of the academic community's involvement in the early histories of COMSEC vs. COMPUSEC. During the infant years of COMSEC devices, large corporations, individual inventors and entrepreneurs, and the government were all involved -- at times even interactively. But the academic world, admittedly less pervasive in those years, generally was not.¹¹⁴ In contrast, the academic and research communities are very much in evidence in any bibliography of early computer security work. Some of the interest on the part of these communities can perhaps be traced to the Ware Task Force of 1967. Not only did the Task Force include members from both communities, but it specifically outlined areas of needed further research.¹¹⁵ From whatever cause, the academic and research communities did indeed become involved and, finding some computer security projects both challenging and useful, many stayed involved. Because researchers rarely view their own work as classified and because of the strong incentives within their community to publish, a pattern of open publication was quickly established.

On the philosophical side, the lack of accord regarding secrecy may proceed from a fundamental disagreement over the nature of the two problems. At the core of the disagreement are differing views as to whether or not computer security is probabilistic in nature, like

COMSEC, and therefore not susceptible to proof of security, or if it is algorithmic and therefore is amenable to analytic solution or proofs of security.

The principal reason for secrecy is to gain and retain a comparative advantage over the adversary. The less the adversary knows about a security system, the more difficult his task, and the longer it is likely to take him to penetrate it and gain useful intelligence from it. But if a system could be proven to be impenetrable, then there would appear to be nothing to be gained from secrecy. Many computer security researchers came to view COMPUSEC as something that could indeed be established by formal mathematical proofs. If true, this would set it apart from COMSEC. Schell makes this distinction explicit when he notes:

. . . cryptography fundamentally depends on probabilities. [It] does not have closed form sufficient conditions. In spite of the research in NP Complete¹¹⁶ and all of that, the state of the art today is that I cannot look at the algorithm and say it is sufficient to meet a definitive measure. And so we develop what are really probabilistic measures Computer security technology is very much of a different kind. It is algorithmic. It depends on proofs (that are real proofs) of sufficiency -- a completely different kind of base.

According to Schell, this difference carries with it profound implications. Says Schell:

. . . the probabilistic base [of cryptography] almost demands that some significant portion of the protection depends on secrecy. [One has] . . . to protect the key; I might want to protect the algorithm The algorithmic base doesn't depend on that at all. It says, ". . . give me your algorithm. I'll submit it to my verification tools. You can try all the attacks that you want, [but] you're not going to slip anything by me. . . ." ¹¹⁸

Schell expounds on this in an article that appeared in an Air Force magazine. He wrote:

The technical breakthrough was the discovery of a set of model functions and conditions that are probably sufficient to prevent compromise for all possible nonkernel computer programs. . . . Security theorems have been proved showing that . . . the kernel will not permit a compromise, regardless of what program uses it or how it is used. That is, the kernel design is penetration proof -- in particular to all those clever attacks the kernel designers never contemplated.

This is an extremely powerful statement. One of the basic and often misunderstood problems in establishing security is that it is not so much a matter of proving that a given system does all that it is supposed to do. Rather, it is the vastly more difficult matter of proving that the system does not do anything it is not supposed to do. The first is a finite task; the second is infinite. The power of Schell's statement is that it asserts that a finite set of model functions and conditions has actually been found that is equivalent to exhausting an infinite list.

This argument certainly suggests that absolute computer security is achievable. Schell is careful to point out that this is true only within what he calls a "confined universe of discourse" but he includes within his universe of discourse all hardware and software controls -- namely those things that "people commonly mean by computer security." Although he does not specifically include within his universe of discourse physical security, personnel security, or administrative security, Schell maintains that if the hardware-software job is done right, the system should still be immune from unauthorized penetration or subversion. As Schell says, "If a programmer writes a bad piece of software, when I submit it to verification, I'll find it."¹²⁰ Schell's ideal COMPUSEC system would not prevent the physical stealing of a

computer disk, but would prevent the unauthorized access of that disk from a terminal.

Schell's computer security system places a great deal of faith in verification. Some others have backed away from this faith. Woodward explains:

I think, historically, the computer security community, when they started thinking about verification, originally tended to fall in the trap of thinking of it as being an absolute thing. If you can verify it, it doesn't matter if everyone has the code of the kernel or whatever. They can't penetrate it because we've proved that there are no holes in it . . . and if you really believe that, then there's no reason not to give out the code

Woodward makes it clear that he does not see verification or security as an absolute thing. "It's not true that there is absolute security," he says, "so I think . . . we shouldn't be as open as we are as far as security goes."¹²¹

How many researchers actually believed that absolute security was achievable is impossible to say. Many would have placed a sufficient number of conditions on their premise that it would have been unclear whether they actually believed it or not. Still, the language that they used created the impression to less discerning readers that they believed that security was a "binary-valued attribute" -- that a system could be said (and proven) to be secure or not secure.¹²²

A more prevalent opinion today is that expressed by Gerald D.

Cole:

Overall security can never be absolute, nor can the accreditation of any individual security mechanism be determined with complete certainty. Even with the use of "proof of correctness" techniques, we can never be completely assured that the proof itself is correct, or that an implementation necessarily matches the more abstract primitives of such a proof."¹²³

Even Schell admits that, although it is theoretically possible to achieve "absolute security," it has not yet been done and will not be for some time. Schell states:

. . . although I might have the technology foundation to do it, I haven't done it, and I'm not going to do it, for some fairly long period of time on any widespread basis
124
. . . .

In the end, then, the advocates of secrecy would seem to have the better case with respect to the absolute security argument.

There is another dimension to the argument over secrecy. Secrecy, and the classification system that makes it concrete and enforceable, is fundamentally a way of restricting access. A security clearance, required for access to classified information, relies upon a security investigation. As a general rule, the higher the clearance, the more thorough the investigation. The purpose of the investigation is to supply information that, in turn, if positive, increases the confidence in the security reliability of the individual. If there is a serious character flaw in the individual, the investigation should reveal it. The entire process, then, is a form of risk management. It seeks a degree of prudent risk by attempting to match the level of personnel security risk with the level of access.

To understand what this has to do with the argument over secrecy, it is necessary to know something about the classes of threats an information system might face. On the most general level, threats can be active or passive. A passive threat involves no aggressive action on the part of an opponent. Examples might be the interception of a radio transmission or the collection of a compromising signal radiated from a cathode-ray display terminal. In these cases the signals are present in the electromagnetic spectrum. An opponent has but to

situate himself favorably and collect the signals. Active threats are of another kind. Against a communications subsystem, they might include such acts as jamming, tampering, stealing key, or spoofing. Against the computer portion of an information system, active threats are usually classed as either acts of penetration or acts of subversion. Since knowing the distinction between penetration and subversion is sufficient to understand the key issues involved in the secrecy argument, the other specific forms of active threats will not be discussed in further detail.

The difference between penetration and subversion is profound. The term "penetration" is usually used to describe those attack strategies that can be carried out even if the system performs as it was originally designed to perform.¹²⁵ Penetration may take advantage of a design oversight or a design flaw, but it deals with the system as it was designed. Subversion, on the other hand, involves a deliberate, surreptitious alteration of the system by an opponent to his own advantage.¹²⁶ The subverter changes the system so that it is no longer the system as intended. The subverter's alteration could be to hardware or software and could be done at any time during the system's life from the earliest stages of design to the last day of its use. It could be done to the original version of the system or to any change or update. The opportunities are endless and the opponent need succeed only once.

The connection between access restriction, imposed by a classified environment, and the threat of subversion should now be clear. One way of attempting to offset the threat of subversion is through tighter access restrictions. If the only persons who are ever in contact with

a system's innards are cleared people, the risk of subversion should be reduced. The extent of the reduction in risk depends upon the effectiveness of the clearance procedure.

What the government is interested in here is a controlled environment -- one in which physical access to the system's hardware and software is restricted to persons who have been thoroughly investigated and found worthy of trust. The government is not so concerned about someone learning some classified fact or walking away with some sensitive information as it is about someone implanting a bug -- some illicit means of future access (called a trap door) -- or, in other words, adding something that is not supposed to be there. The classification system was never designed for this purpose, and in fact, is not even particularly well suited for this use. Classification, even of an entire project, rarely extends to components; yet, components may be the greatest source of risk.

Still, the government seems to have found no better way. In spite of the long-time awareness of this problem, the government's only means of requiring the investigation it wants is classifying the project. Thus, people who believe that the threat of subversion is real tend to argue for a classified environment. Those who do not accept subversion as a realistic threat generally argue for openness.

Perhaps the strongest argument advanced in favor of an open sharing on an unclassified basis is the argument that unless this open sharing is allowed, the government and whoever else might need COMPUSEC mechanisms will have to wait an unacceptably long time for them and may not get them at all.

First, there is the economic factor. It costs money to establish and maintain secrecy. This drives up the price of any security mechanism, which in turn, inhibits the sale and therefore the widespread use of that mechanism.

Second, there is the argument that no one person, no one organization or institution, has a monopoly on all of the ideas that will be needed. Neumann, for example, states:

I think it's absolutely vital that the community recognize the need for really top flight minds -- whether it's academic or industrial or whatever -- but people with some kind of global vision that transcends just the details of the specific system, and you don't find many of those. They're few and far between.

Neumann believes that, in such a situation, it is important to involve academe. While admitting that "there are many academics who are so narrow that they're useless," Neumann also states that most of those with a "global vision . . . tend to be in academia."¹²⁷

Classification, in Neumann's view, is an impediment to the involving of the academic and the research communities. "The experts tend not to be cleared," he says. Another disadvantage of classification, according to Neumann, is that some developers, realizing that few outsiders will get a look at their classified systems, "hide under the mask of the clearance" and produce "pretty shoddy systems."¹²⁸

Yet, even those who advocate open sharing with industry and academe recognize the need for limits. Neumann, for example, concedes that results of counterpenetration studies and of formal verification efforts that show where the unfixable flaws are, should be kept sensitive.¹²⁹ And Dr. Gerald P. Dinneen, when he was Assistant

Secretary of Defense for Communications, Command, Control and Intelligence, stated:

We are going to have to draw a fine line between the openness with which we discuss computer systems development in general and the information restrictions we use to protect the potential vulnerabilities that may exist in the integrity measures of a particular system. We will have to develop procedures for protecting security relevant design and implementation details while not inhibiting general technical advances. 150

In addition to permitting the pursuit of different strategies, several other considerations seem to argue for a continued separation between COMSEC and COMPUSEC, at least for the next several years.

In the first place, there is the matter of inertia. It is almost always easier to continue in the same direction than it is to change course. And it is important to keep in mind that the current separation exists not only within the government but within industry as well. As later chapters show, convergence of the two fields will not be easy. Thus, the burden of proof would seem to fall to those who would argue against continued separation.

Next, there is the matter of complexity. Whenever one faces a large complex task (and information security is certainly such a task), a very logical first step is to break the job down into smaller chunks. As one book on computer networks puts it:

In any complex system design problem the first and critical step is to break down the system into subsystems which can be designed separately. Success depends upon the right choice of functions for these subsystems in order to minimize the complexity of the interface. 151

Dividing the information security job is simply one way of contending with the problem of complexity.

In addition, there are many who see the two problems, as well as the two technical disciplines which have developed to pursue them, as

fundamentally different. (Some of this perceived difference was discussed earlier in the chapter.) Further, since the problems are inherently difficult, each demands a high level of technical competence to succeed. To force the two fields together would be tantamount to requiring practitioners in each field to become proficient in the other. Increased breadth generally comes only at the expense of decreased depth, a prospect almost universally eschewed by highly competent technical people bent on remaining so. There is also the fear that a merging of the two problem areas would require the adoption of a different strategy, and both sides are comfortable with their current strategies and with the environments their strategies create.

There is, finally, the "NSA issue." Eliminating, or even reducing, the current separation between civil and military or between COMSEC and COMPUSEC will almost surely place a larger slice of the entire problem in the hands of the NSA. Even a casual review of Figure 1 in the previous chapter should make this obvious. Within the federal government, NSA clearly enjoys the dominant position in the field of information security. It would certainly be difficult, in the name of centralization, to justify taking any of NSA's current responsibilities away. In fact, the course that would appear to be more logically directed toward greater consolidation would be to give NSA more of the chart's listed functions. But such a move is very likely to meet considerable resistance -- no matter how "logical" it might appear to be.

When PD-24 attempted to assign COMSEC-related functions, NSA was an issue.¹³² Then, the concern was over NSA's other mission -- intelligence. A newspaper article reported at the time:

. . . one congressional staffer said asking NSA to develop security systems for non-military communications was like hiring a burglar to guard the family jewels.¹³³

NSA became an issue again when the DoD sought a location for its Computer Security Evaluation Center. According to Schell, part of the reason for the Air Force's procrastination in agreeing to the draft charter was the fact that the center was located at NSA. Some of the hesitation (see Chapter 6, p. II-86) was due to a natural reluctance to give up any measure of budget control to a competing DoD component. It was a simple case of protecting one's own turf. Some hesitation, too, was the result of some unpleasant past relationships. The Air Force was still smarting over an earlier incident in which a supposedly joint Air Force-NSA COMSEC project had been suddenly "grabbed from them . . . and the door slammed" just as the program was about to enter production. Even worse, in the eyes of the Air Force, was that after having wrested control of this much needed program from the Air Force, NSA allowed the program to languish. According to Schell, "five years later, it was still not on contract."¹³⁴

And there was a third, more substantive reason as well. There is a genuine concern that NSA's unique physical and personnel security environment causes NSA to be insensitive to the problems that the rest of the DoD faces. Schell explains:

. . . NSA can live in a closed, System High¹³⁵ environment and therefore doesn't have a lot of motivation for multilevel solutions. NSA just doesn't face the problem of a computer system which -- in order to be effective [i.e., operationally useful] -- has to have uncleared users.

NSA, says Schell, does not "operate in an environment that includes the threat of KGB agents tapping a line and being on your computer" Yet it is precisely such a threat, according to Schell,

"which the rest of the GENSER [general service] community has to face"136

Finally, there was a deep concern within the services that NSA would overly classify technical work in the field and that this would impede the overall COMPUSEC effort, which they perceived required "the active participation of academic and other industry researchers."¹³⁷

As persuasive as all these arguments are in support of continued separation, there are also compelling arguments against it. Those who argue against continued separation argue principally on the basis of risk. As Peter G. Neumann of SRI International puts it:

There is a decided element of risk resulting from the COMSEC community seeking solutions independently of the COMPUSEC community, and vice versa.¹³⁸

The risk involves the distinction, common in mathematics, between the notions of necessity and of sufficiency. No one argues that both COMSEC and COMPUSEC are not necessary for the overall security of an information system. The argument is over whether or not the attainment of both, along with the other securities such as physical, personnel, and administrative, is sufficient for information security. A 1978 Air Force report prepared by the MITRE Corporation said it was not. The report stated:

Although computer networks evolved out of the union of communications and computer science, their security issues are more than the simple union of the security issues of communications and computers. The problems in both areas combine and new problems emerge from the interactions between multiple computers and communications lines.¹³⁹

The risk, then, lies in these elusive "new problems." The fear is that when one tries to divide up a system into COMSEC and COMPUSEC pieces, he will create some new crack through which information will leak. If such a crack results, it is apparently not well understood

and would be difficult to describe. Nevertheless, its very importance seems to dictate that we make an effort to understand.

A review of recent literature in both the COMSEC and the COMPUSEC fields reveals numerous references to the term network security.¹⁴⁰ Although rarely defined, it is usually clear from the context that network security, while embodying the concepts of both COMSEC and COMPUSEC, offers some "value added" of its own as well. Perhaps the most explicit enunciation of network security can be found in a paper presented at the 1979 Computer Conference by three persons who were then working for the Ford Aerospace and Communications Corporation. It says that a secure network can be considered to be composed of two elements -- hosts or subscribers, and a data communications subnet. The paper then states:

We assert without further argument that a network (Host and subnet) can be considered secure if:

- . Multilevel network Hosts properly protect data while the data is resident within the Host and properly label data with its classification when submitted to the communications subnet for transmission to another Host.
- . The communications subnet restricts unilevel Hosts to receive and transmit only data labelled with the classification each is permitted to process.
- . The communications subnet maintains the integrity of transmitted data, particularly its classification label.
- . The Confinement Problem¹⁴¹ is suitably dealt with, either by policy decision or by means detailed below.
- . Communications lines are protected from compromise or modification (usually through encryption).¹⁴²

Setting aside the important question of whether the above list of five characteristics is complete or sufficient, we can examine each characteristic to determine if it could reasonably be expected to be

dealt with through normal COMSEC or COMPUSEC measures or if it seems to demand something beyond the normal scope of both.

The first characteristic is a basic expectation of computer security. Proper protection and labeling of resident data are fundamental properties implicit in the notion of a trusted computing base. The third and the fifth characteristics should be provided by any communications system that has been carefully designed from a COMSEC standpoint. The achievement of integrity may require authentication, but COMSEC can provide this. The second characteristic appears to be achievable only by incorporating a trusted computing base (TCB) within the communications subnet. In fact, the same paper goes on to describe what its authors call a communications subnetwork processor (CSNP), a TCB which, among other things, performs the labeling function:

For Hosts without multilevel security, the CSNP must "know" the current level of operation. For Hosts with multilevel security, the Host is trusted to label each transmission to the CSNP. In both cases, the code that manages the Host-CSNP interface resides within the CSNP's kernel.¹⁴³

The second characteristic, then, appears to be achievable so long as one is willing to combine COMPUSEC and COMSEC within the communications subnet.

This still leaves the fourth characteristic, the confinement problem. For a system to have a "confinement problem," some channel or path must exist from the trusted to the untrusted domain. Such a channel is usually referred to as a "covert channel." Confinement is generally considered to be a computer security problem. (Covert channels are acknowledged and defined in the CSEC's evaluation criteria document.¹⁴⁴) But like the labeling problem, confinement must be

handled within a CSNP for the subnet to be secure. Unlike the labeling problem, however, there is no ready solution to the confinement problem. No one claims to know how to eliminate all covert channels, short of destroying all useful functionality of the system -- a concrete example of the security dilemma of Chapter 1. The only suggested measures for contending with covert channels call for determining and restricting their bandwidth and for rendering them noisy.¹⁴⁵

There is one last aspect to the argument over separation, which may be the strongest factor of all. It concerns the matter of organization.

To attempt to maintain the separation between COMSEC and COMPUSEC will require some way of making functional distinctions that can be used to determine the organizational assignment of a particular problem. As communications systems grow increasingly complex, these functional decisions are likely to become increasingly arbitrary and artificial. This is exactly the same problem that confronted the NTIA when it tried to devise definitions that would distinguish between national security and non-national security related information. The distinction between the COMSEC and the COMPUSEC features of a modern teleprocessing system is just as fuzzy and any attempt to define it is sure to yield equal frustration.

On the other hand, a decision to integrate the two functions could easily lead to an inappropriate subjugation of one function to the other, depending upon which side ends up in control. Inman seemed to sense this danger when he chose to establish computer security as a separate organizational entity within the NSA.¹⁴⁶

This risk of inappropriate subjugation results from a somewhat understandable tendency on the part of both COMSEC and COMPUSEC practitioners to have a limited view of the other field -- even to view the other field as a subset of his or her own.

A person accustomed to dealing with the problem of securing large telecommunications networks is likely to envision two different kinds of computers -- those which assist in the network management functions and those which sit at the tails of his network and appear to the network as terminals. This latter kind is not substantially different, from such a person's point of view, from most other forms of "smart" terminals including a simple telephone that can "remember" what number it dialed last. The terminal, be it a telephone or a computer, is simply the user's interface with the telecommunications network. If reasonably enlightened, our COMSEC practitioner probably does see computer security as a concern with which he must deal in order to achieve communications security. He would understand, for example, that if an opponent could penetrate the network management computer, COMSEC has not been achieved. In other words, he sees COMPUSEC as an important ingredient -- and thus, a subset -- of COMSEC.

Further, he is quite likely to think in terms of physical protection of the computing resource, since COMSEC has traditionally relied heavily upon physical protection of both cryptographic devices and their keys. If so, he fails to appreciate what is perhaps the most fundamental of COMPUSEC notions, namely that the very people COMPUSEC seeks to protect against are those who have legitimate access to the computing resource.

Alternatively, one who has been engaged in trying to secure large, complex computing or processing systems -- systems typically consisting of internettted computers that share computational capability, data files, or both -- is likely to have quite a different view of the COMSEC-COMPUSEC interrelationship. Such a person is likely to see the computer network as simply a natural extension of the concept of remote access, and distributed processing as an extension of time sharing -- differences, not of kind, but of degree. Vinton G. Cerf writes:

. . . communication has always been an essential component of digital computing. The internal architecture of computers involves the movement of data from one part of the system to another Remote access to computing resources via distant computer terminals . . . has also played an important and increasing role in the design and provision of computer based service.

Such a person is quite likely to view communications protection of all interconnecting links as vital, but he is also quite likely to assume that such protection can be achieved by the relatively simple expedient (and common practice) of "hanging" a cryptographic device on both ends of every link. This, as any COMSEC professional will tell you, is a naive notion. Full communications protection must include proper key management, careful start-up procedures, analysis and attention to hardware failure tendencies, and emonation control, among other things. Our computer-oriented individual is guilty of the rather widespread tendency among non-COMSEC people to equate COMSEC with cryptography -- something a COMSEC insider would never do.

Thus, both the COMSEC and the COMPUSEC professionals acknowledge the importance of the contribution of the other field. Both consider the other necessary. But both may also consider the other subservient -- not in any pejorative sense, but in an operational sense. And, of

course, this view might color either person's organizational decisions were he or she allowed to make them.

We seem to be left in somewhat of a dilemma. There are certainly any number of compelling reasons for maintaining the current separation between COMSEC and COMPUSEC -- particularly in technical organizations. In fact, as has been stated, integrating them might be extremely difficult and perhaps achieved only at the price of inappropriate subjugation of one to the other. On the other hand, this chapter has claimed that as systems become more and more complex and as some of the "network security" issues begin to dominate, attempting to maintain the separation is likely to lead to artificial distinctions and ultimately runs the risk of achieving neither COMSEC nor COMPUSEC. Before we can assess the seriousness of this risk, we need to understand better just what is it that is at risk and the nature of the threat against it.

Chapter 9

Risks, Interests, and Markets

In order to reach any conclusions regarding the seriousness of the separateness debate or the importance of its outcome, it is necessary to appreciate what is at risk. And to assess how likely a particular outcome might be, it is useful to have some idea of the stakes and interests of the various players who will probably determine the outcome. If either of the two sides in the debate is right, and it makes a difference whether COMSEC and COMPUSEC are pursued separately or together, then the security of the information within the system could be at risk. Even if both sides are wrong and the security of information is relatively unaffected by the strategy chosen, there are other stakes that some individuals and organizations perceive as important. For instance, there are economic interests for those companies that might or might not be able to respond to the stated requirement, depending upon the outcome of the debate. Just as the outcome of the debate could affect some of the players' interests, the players' perception of the interests could affect the outcome of the debate. For example, the outcome of the debate will influence the market for secure products, but the perceived market is having quite an influence upon the debate as well. In this chapter, we examine some of these risks, interests, and markets.

The largest single user of computers in the United States is the federal government.¹⁴⁸ According to a 1981 report by the Rand Corporation, the U.S. government operated 15,142 computers in fiscal year 1980, an increase of nearly 80% over the 8649 used in fiscal year

1975.¹⁴⁹ Both the national security and the civil sectors of the U.S. government are entrusting a considerable amount of information either to internettted computer systems or to computer-aided communications systems. The national security sector employs such systems as the World Wide Military Command and Control System Intercomputer Network (WIN)¹⁵⁰, the Department of Defense Intelligence Information System (DODIIS),¹⁵¹ and the already mentioned intelligence network, COINS.¹⁵² All involve networks of computers and complex communications subsystems. In his keynote address to the Fourth Seminar on the DoD Computer Security Initiative, Admiral Bobby R. Inman, Deputy Director of Central Intelligence, made specific reference to ". . . the growing use of automated information handling systems throughout the DoD and the Intelligence Community and in particular the linking of these systems into major networks."¹⁵³

As the use of internettted systems increases and as networks enlarge and proliferate, the potential for mischief multiplies. Whether this potential is realized in fact depends upon whether or not there exists some adversary who is properly situated and sufficiently motivated and capable to attempt a penetration or interception.

Within the national security sector, a central assumption is that there always exists a highly motivated, well financed, and technologically sophisticated opponent who is engaged in a constant search for targets of opportunity. As a general rule, the most worthy opponent of the United States is considered to be the Soviet Union's KGB, which, according to former Soviet diplomat Arkady Shevchenko, is the sole Soviet organization that has "no limitations whatsoever" placed upon the money it spends and whose spending is checked by no one

outside the Politburo.¹⁵⁴ That the Soviet Union is probably sufficiently motivated and may be technically sophisticated enough to accomplish computer penetrations was indicated in two ways: by its illegal accessing of a CRAY-1 computer at the University of Reading in England, which, according to Parade Magazine, it then used to make complex calculations for its nuclear weapons design; and by its ability to access U.S. data bases illicitly. The Soviets reportedly accomplished both of these by way of the computer links of the International Institute for Applied Systems Analysis near Vienna.¹⁵⁵

Although the chief foreign threat is the large number of officially accredited diplomatic personnel assigned to embassies, consulates, and the United Nations, some among the large number of foreign visitors to the U.S. may also represent potential threats. According to William Webster, Director of the Federal Bureau of Investigation, more than 82,000 persons from Soviet and Soviet-bloc countries entered the United States during 1981. In addition, there were approximately 33,500 visitors, tourists, and immigrants from the People's Republic of China.¹⁵⁶

It is not only the national security sector of government that has a stake in information security. Civil agencies, too, have much at risk. NBS' James H. Burrows made this point at a 1981 conference:

Computer security is no longer an exclusive concern of the defense and intelligence communities As we become more dependent upon computers for handling financial, health and other critical information, techniques for assuring the integrity and reliability of computer systems become essential throughout the government and private sectors.¹⁵⁷

Not all of these computers are independent or stand-alone systems, either. In a 1982 report the General Accounting Office (GAO) stated that it was aware of 31 dedicated telecommunications networks used to

support the computers of the civil agencies.¹⁵⁸ The GAO report further stated that as civil agencies "expand their use of telecommunications networks, their information systems will become even more vulnerable" unless senior management devotes more attention and resources to information systems protection.¹⁵⁹

That these computers and computer networks are not immune from malicious penetration is clear from another GAO study, this one performed in 1976. According to this earlier study, in spite of an admitted difficulty in acquiring data on computer-related crime, the GAO was still able to turn up 69 crimes or incidents resulting in losses of over \$2 million.¹⁶⁰ In the 69 cases studied, most involved unsophisticated methods and most were committed by persons within their own work environments.¹⁶¹

This second finding was confirmed by a 1983 survey of computer-related fraud and abuse in government agencies. The 1983 survey concluded that almost two-thirds of the fraud perpetrators were functional users of the system. Another finding was that 65% of the fraud cases involved only one person, which means that a shocking 35% involved the collusion of two or more persons.¹⁶²

The private business sector, too, has become increasingly dependent upon interconnected computers. Banks use them to transfer funds; airlines use them for reservations and bookings; offices use them for electronic mail; service organizations use them to transfer information on services and clients; and newspapers use them for decentralized printing. According to the earlier cited Rand study, the assets that are stored in computer systems "and thus exposed to security risks include financial records, information necessary for

business functions, trade secrets, and marketing data."¹⁶³ And, as one writer notes, as computers are used to control more and more functions, "the potential for computer abuse multiplies."¹⁶⁴

Business information cannot be assumed immune from the attention of the Soviet Union or any other foreign adversary. There have been suggestions that the U.S.S.R. has made use of communications intercept information to manipulate commercial markets -- during the 1974 grain deal, for example.¹⁶⁵ And it is quite possible that another country's strategy might embrace more than just passive interception. Schell, for example, notes that were he the foreign opponent, he would view "the ability to totally disrupt and neutralize our financial system" as forming an important part of his overall strategy.¹⁶⁶

Even apart from any foreign threat, Rein Turn, author of the Rand study, points to four generic reasons for attention to COMPUSEC on the part of the private or business sector. These, he lists as protection of assets and resources, regulatory compliance, management control, and safety and integrity. He also notes that the use of trusted computer systems could offer economies of operation, advantages in the marketplace (particularly to financial institutions), and enhancement of a company's public image.¹⁶⁷

The safety and integrity advantages of trusted systems, according to Turn, accrue from careful methodology involved in their development and from the attention given to their continued integrity. Turn cites the efforts to verify correctness of the software, efforts mandated for higher levels of trusted computers, as contributing significantly to effective management control.¹⁶⁸

With regard to regulatory compliance, Turn points out that many state corporation laws and federal Security and Exchange Commission (SEC) regulations require computer security, not explicitly, but by implication. He also notes that federal laws such as the Fair Credit Reporting Act of 1969, the Family Educational Rights and Privacy Act of 1974, and the Financial Privacy Act of 1980 all contain clauses that have strong security implications. Finally, he notes that several European countries and Canada have enacted privacy and data protection laws that particularly affect any company storing personal information on any of those countries' natural or legal persons.¹⁶⁹

Protection of assets tends to be a straightforward economic consideration. There is certainly a great deal at risk. According to an April 1981 article in Business Week, "banks use . . . communications links to transfer electronically more than \$400 billion daily."¹⁷⁰ Nor are losses negligible. In the 100 or so cases of computer crime reported each year, losses run about \$100 million. Most computer crimes go unreported. As Leslie S. Chalmers of the Bank of California pointed out at a 1983 conference:

Most companies . . . are quite reluctant to discuss specifics about computer crimes they may have suffered The reason for that is . . . each company does not want to be perceived as being vulnerable. It's bad for public relations. And the other thing is it would encourage other people to come and try at it, too. If they know somebody succeeded in ripping off a bank, they might hit that bank. It's human nature.

Estimates of computer crimes not reported run as high as 3 or 3.5 billion.¹⁷² Some indication of the level of concern can be found in two related facts. First, the above-cited Business Week article estimated that businesses would spend \$150 million in 1982 for computer security services, ten times the amount spent five years earlier.¹⁷³

Second, several companies now offer insurance protection against losses from computer fraud and theft.¹⁷⁴

Much has been written about computer crime. Both the popular press and the technical literature abound with tales of computer-assisted larcenous exploits -- some simple-minded, some exceedingly clever, but almost all highly profitable.¹⁷⁵ The public seems to have a high tolerance for -- even a fascination with -- such tales.

Undoubtedly, many computer-related crime cases are never detected. Of those detected, as was stated above, most are generally conceded to go unreported. But even among the cases reported, one is struck by the number of instances in which the perpetrators, even when caught, are never prosecuted. Perhaps the most bizarre such story came from a computer security consultant and was reported in the August 1982 issue of Smithsonian magazine:

Another case that never came to trial . . . occurred last year at an East Coast bank. The employee had stolen about \$8 million by the time his activities were discovered. Over breakfast at a local restaurant, bank officials confronted the man. Look, he told them, if you prosecute me, then the details about the flaws in your data-processing system will become public knowledge -- and it will cost you a lot more to fix the system than you're losing to me. The bank officials reluctantly agreed, and simply asked him to resign. "I'll keep the eight million," he said with a smile as he got up¹⁷⁶ to leave, "but I'll pick up the tab for breakfast."

This case points up not only the relatively low-risk environment many would-be computer thieves face, but also the magnitude of the technical problem. Any problem, limited to a single bank, that will cost more than \$8 million to fix, is no small problem.

Not only are many computer thieves not prosecuted, but some are even given good references by their employer, anxious to be rid of them. The following story came from Congressional Quarterly:

An extreme example came in the case of a young executive in England who, when confronted with evidence, admitted he had been stealing from his company's computer. For fear of bad publicity, the company gave the man a letter of recommendation to help him find a new job. He soon went to work for another company, embezzling some \$2,000 a week for three-and-a-half years. For a second time, the embezzler was uncovered but not prosecuted. Again the victimized company did not ask for restitution¹⁷⁷ and provided the thief with a good employment reference.

Interest in computer crime among law enforcement authorities is high. According to an October 1982 article in Business Week:

The Federal Bureau of Investigation has set up a school of computer crime, but it says it cannot handle all the requests¹⁷⁸ from state and local authorities who want to attend.

A common complaint among law enforcement officials is that present laws were not written with computer crime in mind and are inadequate as a basis for the prosecution of many computer-related offenses. For this reason, beginning in 1977 a series of bills have been introduced in Congress aimed at easing the prosecution of the computer criminal.¹⁷⁹ In making the case for new legislation, one lawyer wrote:

These bills and laws make it no longer necessary for prosecutors to "shoe horn" their cases into statutes and case law, which neither considered the technical complexities of computers, nor the kinds of criminal acts which involve computers. The severe procedural and evidentiary handicaps which have so often accompanied the use of¹⁸⁰ existing laws are not obstacles under these bills and acts.

During the 98th Congress (1983-84), the designation of these bills were H.R. 1092 in the House of Representative and S. 2270 in the Senate. They would have made it a federal offense to tamper with government computers, those involved in interstate commerce and those of financial institutions whose assets are insured by the government.¹⁸¹ Neither of these bills passed, but in the closing days of the 98th Congress, "The Counterfeit Access Device and Computer Fraud Act of 1984" was enacted

as part of a continuing appropriation bill.¹⁸²

The 1984 law prohibits unauthorized access in the following three specific instances:

1. if the perpetrator intends to harm the United States or has reason to believe that such harm would result.
2. to obtain records held by either a financial institution or a consumer reporting agency.
3. to knowingly use, modify, destroy or disclose information in or to prevent the use of a computer operated by or on behalf of the U.S. government.¹⁸³

Beyond this particular law, however, there has not been overwhelming support for general computer crime legislation at the federal level.¹⁸⁴

In fact, not everyone agrees that such a law is even necessary. A few legal authorities have come forward to argue that, with proper allowance for intent, present laws can be used and used effectively to prosecute computer related crime. Roy Freed, an attorney who is widely credited with having pioneered the field of computer law, is one of those who believes that wholesale changes in the law are unnecessary to accommodate modern computer technology. In fact, he has made a successful career out of fitting the ever-changing computer technology into the framework of existing law.¹⁸⁵ And Robert Ellis Smith wrote in a 1982 article for Datamation:

It was fashionable in the 1970s to say that the old legal principles developed before the age of electronics were inadequate to govern the automated information society. But perhaps we are discovering¹⁸⁶ in the 1980s that the old principles still apply.

It is quite possible that both sides are right. That, according

to a March 1983 article in Computerworld, is the opinion of Harvard Law School Professor, Arthur Miller. Miller believes, says the article, "that the current legal structure is capable of handling computer-related crime." As the article points out, however, "this does not mean laws specifically related to computer crime should not be passed." The article goes on to quote Miller as stating that the passage of computer-specific legislation

would help by cutting the mumbo-jumbo metaphysics [for example], whether theft statutes apply to information, and prevent lawyers from playing their little games and it would have a tendency toward a psychological factor to say, for example, "There is no doubt that stealing from computers is like stealing from humans. . . ." ¹⁸⁷

Passage of specific legislation would probably also clarify the matter of liability. What is not clear is the extent to which a custodian of information is responsible for its safeguarding. Statutes and legal precedent exist that would permit an injured party (someone whose personal data has been lost or misused) to sue a custodian when that custodian deliberately sells or otherwise misuses privacy data entrusted to him. ¹⁸⁸ There would also appear to be grounds for suit on the part of an injured person against some third party for stealing the data from the custodian. But a search for cases in which an injured party has brought suit against the custodian when the actual theft of data has been made by a third party, proved fruitless. Such a suit, of course, would allege that the very fact that a third party was able to steal the data should constitute prima facie evidence that the custodian's security control was inadequate. ¹⁸⁹ The appearance of such a case would seem to be only a matter of time. Reflecting the opinion of Professor Miller, the Computerworld article states:

Precedent-setting court cases will come in time, according to Miller. In a case in which someone has been wronged because an institution failed to safeguard properly its data, the issue would be whether a normal, reasonable duty exists to safeguard data. And the day the decision comes down, all systems worth their salt¹⁹⁰ will upgrade their security to ensure their survival.

Wholesale security upgrading, however, is not the only possible outcome. Should a few of the settlements be large, it is not hard to imagine a situation developing similar to that within the medical profession when malpractice suits became popular. Just as physicians demanded malpractice insurance, data custodians facing an uncertain number of possibly costly suits might demand penetration insurance. Ironically, if this were to occur, the demand for security enhancement mechanisms might actually diminish in the short run. A custodian might consider insurance to be a much better investment than security enhancement. After the cheap and easy enhancements have been made, additional improvement in security will quickly become quite expensive (requiring, for example, discarding the present system and starting over) and even if a rather substantial investment were made, the custodian might still have considerable difficulty convincing a jury that his protection was adequate when some third party had been able to penetrate it. In the longer run, the pressure for additional security mechanisms might take the form of reduced penetration insurance premiums for those custodians whose information systems were judged to meet some industry standard. (Premiums for other forms of insurance such as against fraud already take note of security features.) For this entire scenario to play itself out would likely take several years, but it seems quite plausible.

Malpractice suits alleging inadequate computer protection might

not be directed only against custodians. They could be directed against manufacturers as well. This could also hasten the arrival of improved security mechanisms. Stanley L. Sokolik writes:

As time goes on, computer manufacturers will find it more and more realistic to reorder the priorities they have assigned to security in their computers. They will not want to risk being sued as an accessory to crime¹⁹¹ or for malpractice for the programs they provide.

In the absence of either such development, we might ask what is the market for information security products and services. If the vulnerabilities are as severe as they are said to be and if the threat is indeed real, one might expect there to be an unquenchable thirst for any and all such products and services that offered any hope of coping with the vulnerabilities. If there is a giant market out there, then it appears, at least for the present, that the giant is sleeping. One indicator of this market somnolence is what has happened to the DES cryptographic equipment business. A 1981 article in Electronics magazine reported:

When the National Bureau of Standards published the data encryption standard in early 1977, at least eight semiconductor manufacturers leaped to produce dedicated DES chips or chip sets. Additional vendors jumped in at the system level, with black boxes designed to capitalize on what all agreed was to become a booming market for DES chips and equipment.

Unfortunately, that estimation turned out to be grossly in error. Despite the vendors' best efforts, few commercial data-processing managers were convinced of the need to encrypt their data messages, and the expected DES market explosion never materialized.¹⁹²

According to J. Michael Nye, a marketing consultant, "The market for encryption devices should be strong and healthy -- unfortunately, suppliers of products are struggling to survive, even though the need for these products has never been greater."¹⁹³ Instead of a market in the hundreds of millions of dollars, as had been predicted, the market

in 1981 for data, facsimile, and text encryption equipment was assessed at only \$18 million, and estimated to rise only to \$44.9 million by 1991.¹⁹⁴

Several reasons have been offered for this lethargic market. The first and most obvious is cost. According to Lee M. Paschall, President of American Satellite Company, "Cost probably represents one of the most formidable barriers to developing extensive secure communications."¹⁹⁵ And, as consultant Nye points out, ". . . it is difficult to convince users to acquire cryptographic equipment when it may cost several times more than the equipment to which the encryption device is attached."¹⁹⁶ Actually, the cost ratio to which Nye refers is fast becoming less and less representative as the price of cryptography lowers and the size and the complexity of communications systems grow.

A second reason is a lack of user awareness or acceptance of the threat or of the vulnerability. "There is," declares Nye, "a significant lack of user awareness of the problems of electronic interception or the vulnerabilities of the existing communications network."¹⁹⁷ Even if generally aware of the threat, some may not perceive it as serious. Says Paschall:

I think one of the main reasons why the issue has been inadequately and haphazardly addressed is that industry as a whole has not been brought to the realization that a serious problem exists.¹⁹⁸

James A. Schweitzer of the Xerox Corporation echoes the same sentiments:

[T]he business marketplace will respond only as managers see the costs of application of these technologies justified by the perceived risks. The poor market reception of encryption products to date reflects management's general view that the problem is not yet serious. In fact, our own experience has been that most significant losses of information occur via the paper medium.¹⁹⁹

Then there is the matter of priority -- putting first things first. For, as one writer points out, "even when users understand the importance of securing their data processing facilities . . . securing telecommunications is not necessarily the highest priority on the list."²⁰⁰ Harry De Maio, Director of the Data Security Programs for IBM, offers a specific example:

If a user of an information system does not have an access control system, . . . then clearly they ought to get that straightened out first before they start²⁰¹ going after rather elaborate telecommunications protection.

Yet another reason offered is that the prolonged debate on the robustness of the DES algorithm²⁰² has made would-be buyers wary. As Nye puts it:

In some sense, the scientific communities [sic] debate on the Data Encryption Standard (DES) has been counterproductive in the user groups. The unfortunate extensive press coverage of the DES debate concerning its weaknesses to determined attack has given the reader the opinion that the DES is of no value; therefore the user does nothing.²⁰³

Some manufacturers may be discomforted by what they see as an uncertain and a discriminatory foreign trade situation. U.S. International Traffic in Arms Regulations (ITAR) require U.S. manufacturers to obtain an export license for all cryptographic equipment including that embodying the DES algorithm.²⁰⁴ According to Nye, licenses tend to be granted for specific applications only, and not for incorporation into other non-domestic products. As industry sees it, the government may here be speaking with more than one voice. According to IBM's Harry B. DeMaio:

One the one hand, we are being told that we are in an economic war and that economic war and that economic information needs to be protected as it moves overseas. On the other hand, we are being told that the [encryption]

devices that are required to make that protection happen may very often not leave our shores.²⁰⁵

At the same time that exports are restricted, there are no U.S. restrictions on the import of cryptographic hardware. Both of these factors tend to work to the disadvantage of U.S. manufacturers.²⁰⁶ In fact, says Nye:

. . . it appears that [foreign] vendors [of cryptographic equipment] enjoy higher sales volumes in the U.S. domestic market than do our own manufacturers. Even though domestic vendors are experiencing difficulty in achieving respectable sales levels in the domestic market, foreign vendors see the U.S. market as huge The restrictive export requirements combined with very loose or non-existent import regulations regarding cryptographic equipment places U.S. manufacturers at an extreme disadvantage in the marketplace.²⁰⁷

Finally, particularly when employed in large networks, cryptographic protection may not help all that much. It may simply transfer the concern rather than eliminate it. As was pointed out earlier, a cryptographic system is no more secure than its key.²⁰⁸ But proper key management is no easy matter and often imposes "a burden that seems greater than the perceived value of the added security."²⁰⁹ Automatic key distribution is frequently employed to avoid the operational and security difficulties that attend physical distribution. However, this merely replaces physical security concerns, which are well understood but hard to solve, with computer security concerns, which are not usually well understood. Here, the COMSEC-COMPUSEC interdependence is truly revealed. A study performed by SRI International points out:

. . . encryption, considered in the broad context of computer and communications 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 that²¹⁰ are easier and safer than defeating an encryption system.

In spite of a rather inauspicious beginning and all of the above reasons for avoiding encryption, many are still predicting an expanding market for cryptography. According to Thomas J. Mitchell of Analytics, "the market for cryptographic protection seems to have regenerated itself" He states that the financial community, in particular, is behind this "rebirth in interest." According to Mitchell, competitive pressures are forcing financial institutions to consider cryptographic techniques for electronic funds transfer (EFT) systems -- both to assure privacy and for validation. Mitchell points out that every major U.S. bank now has an individual specifically responsible for data security and in 1981 he predicted that "procurement of data security equipment -- will take place at most banks during the coming year."²¹¹ Eb Klemens of Circle Software Corporation agrees. He believes that "encryption is going to be a sleeper" and compares it to access control, which, he says, also had a slow start but for which there has been a "tremendous market demand" in the past few years.²¹²

A 1980 study of the cryptographic market conducted by the Carnegie-Mellon University reached a similar conclusion. The report concluded:

Our surveys and our interviews with current and potential users have convinced us that the current market for data encryption devices is very small and that the rate of growth over the next few years is likely to remain low. . . .

Despite its limited short term market potential, we believe that in the long run, as communications services become ubiquitous and encryption hardware prices decline, the use of data²¹³ encryption technology will become wide-spread.

Also, when evaluating the cryptographic market, a perspective

helps. Cryptographic devices might not be selling at the rate companies hoped or perhaps even expected, but, as Kahn reminds us, there are still more in use today than ever before in history. Kahn writes:

Today, the volume of information that governments, businesses, and individuals store in databanks and transmit among computers is rapidly rising, while the cost of encryption, thanks to microprocessors and large-scale integration of electronic circuits, is rapidly falling. This combination of factors is driving the continued expansion of cryptography, whose use is wider now than at any other time in history.²¹⁴

Measuring the market for computer security mechanisms (trusted systems) is much harder because there have been few products to evoke market response. Computer vendors have been proceeding very cautiously. Rein Turn, in a Rand study of the latent requirement for trusted computer systems, stated:

System software vendors are primarily concerned with whether or not a proposed system will have a sufficiently large market to justify its development costs.²¹⁵

Until a wide market is perceived, there will be few products, and so long as there are few products, assessing the potential market is chancy, as suppliers of cryptography have painfully learned. Turn points out:

. . . the situation is somewhat circular: A market will develop along with availability, but availability is influenced by the size of the market.²¹⁶

There is a natural reluctance on the part of potential suppliers of trusted systems to repeat the mistake, apparently made by their COMSEC counterparts, of introducing products prematurely. This reluctance is only heightened by the relative extent of the underlying risk. The cost associated with developing a trusted computer system is

likely to be at least an order of magnitude greater than that required for an encryption device.

Now that Honeywell's SCOMP has been announced and is available for purchase, other would-be software and hardware vendors may be watching its sales with great interest. As one member of a competing company's staff put it:

I'll be interested to see how they do with it. . . . My impression is that they're getting a lot of evaluation customers. I assume they'd like to sell more than that.²¹⁷

Peter Neumann of SRI believes that if Honeywell begins to have notable success in selling its SCOMP, IBM would attempt to jump in and market a trusted computer of its own. To justify his belief, Neumann points out:

This happened with the IBM Model 67. GE [the original developer of the Multics hardware] wound up with several of IBM's regular customers placing orders for Multics. This seems to have catalyzed IBM into deciding to market a competitive system (360/67 TSS), with the intent that it would do whatever Multics did. It didn't.²¹⁸

IBM's DeMaio is not sure. He states:

[Y]ou've got to remember . . . that our installed user base is already committed to a certain class of architecture . . . I don't know where Honeywell is going to get their market for SCOMP. I don't know when we would find a similar market for a similar device if we went for it. When you do have the type of installed base that we've got and that installed base has the tremendous inventory of existing applications and investments in software . . ., moving off an architectural standard in any major way is something that you really wring your hands over for an extended period of time before you make any efforts, and then you do it in an evolutionary fashion.²¹⁹

Regardless of IBM's response, DEC's Lipner points out that the SCOMP is likely to prove useful in another way: it will help other vendors calibrate the evaluation criteria and process. According to Lipner, the draft DoD criteria are subject to interpretation and one

completed evaluation will serve as a benchmark. He says:

I will be interested to see how their evaluation does. One of the things . . . we desperately need is to see some worked examples of some evaluations -- just to see the intended interpretations of the words in the evaluation criteria.²²⁰

Meanwhile, some computer vendors may be inching their way into the security market by introducing products at the lower end of the security scale first. That, for example, appears to be DEC's strategy. According to Lipner, who is responsible for advanced development of DEC's security products, his company perceives a market among its general class of commercial customers for a product at about the C2 security level, with perhaps a couple of features added from the B1 or B2 class. Regarding a product that would be robust enough to earn one of the higher overall ratings, he says, "There are a lot of things at B2 and maybe at B1 that people do not perceive a need for so clearly."²²¹ Beyond the B1 security class, Lipner perceives a market confined to the government.

Typical business applications do not appear to face the same degree of threat as that found by the government. James A. Schweitzer of the Xerox Corporation states:

For government, security concern is critical and deals with absolutes; that is, matters of defense must have over-riding priorities and large sums can be and are expended. For business, information is one of a number of critical resources which require management attention. Managers make decisions about risk-taking all the time. Security is one of a set of elements supporting the integrity and reliability of business information. Business managers then have a much wider scope of action in determining how much effort (expense) should be expended on information security, or even whether such security is worth its cost.²²²

Although he sees the above-B1 market as limited, Lipner admits that his company is committing resources toward the goal of a

high-security product.

We're doing an advanced development. We perceive . . . that there could be a market -- several major government procurements, say, as a lower bound -- for an A1 or an A2 system.

When asked how soon he thought this market might materialize, Lipner replied: "I believe we could sell them next week if we had them."

And, he added:

We believe that the price is probably not bounded. We haven't come to grips with specific pricing issues. ²²³

In spite of this rather upbeat assessment of the market, Lipner also made it clear that the market for these high-security products is not only limited but uncertain.

I'd like to believe that there would be some number sold. I think that if we kept the development costs low enough, we could make money. But I don't see a situation where every DoD procurement is for an A1 or better system in three years . . . and indeed, as I watch the procurements, I see even the ones that should be [prescribing an A1 system], waffling.

Recalling his own days on the government side of the procurement process, Lipner attributes the government equivocation with regard to security specifications to a fear that no one will be able to respond and the program will lose its funding support. As Lipner puts it:

I believe the main reason they waffle [is that] they perceive that there's nobody out there. . . . If you say you need it and nobody can deliver it, then your program is infeasible and you get turned off. ²²⁴

There is a second reason that potential vendors of high-security COMPUSEC products are proceeding cautiously. Just as with communications security products, there is a concern over exportability. According to Theodore M. P. Lee, the Manager of Systems Security at Sperry-Univac:

[A] lost opportunity cost, of a sort, is the chance that an A1 system would be so good that we would be prohibited from exporting it, (to almost anywhere, not just the Eastern bloc) meaning that by developing a better product we would in fact be losing marketplaces. And I'm sure that we would not be interested in developing a system, especially if we take the risk, that could not be marketed as part of our standard product line to all customers.²²⁵

Thus, computer security products, at least those at the higher security levels (A1 and beyond) that the national security part of the government says it needs for its more sensitive applications, seem to remain several years away. Lee's estimate is between five and ten years.²²⁶

If highly secure products are to be so long in coming, one might ask what effect this is likely to have on the prospective users of such products. To answer this question, we have to address the matter of cost.

Cost shows up in various ways. There is, first of all, the cost associated with loss. In organizations that are able to place a dollar value on potential losses, costs can be examined in a relatively straightforward manner. Cost of protection is compared with the cost of the expected loss. Typically, this is done through the formal device of a risk assessment, which attempts to assign a dollar value and a probability to each and every "bad thing" that can happen.²²⁷ In organizations that face losses that cannot easily be measured in economic terms, determining the cost associated with the loss is not so easily done. As computer security consultant Robert H. Courtney puts it:

It is usually not easy to assess the dollar impact of loss of unclassified data or of processing capability. An even greater problem is encountered when trying to assess the probability of espionage and sabotage.²²⁸

At the same time, in spite of the difficulty, Courtney argues for a risk assessment:

Security measures should be selected on the basis of their benefit/cost relationship. This requires that benefits be quantified for comparison with costs. Risk, too, must be quantified in order to measure the effect of its diminution or elimination.²²⁹

It is undoubtedly recognition of this need for quantification that has led both government and industry to embrace security risk assessment as an important ingredient in their overall information security programs.

But costs can show up in ways other than loss. Nowhere is this felt more keenly than within the DoD, whose component organizations are forced by regulation to compensate for a lack of computer security by means of costly administrative controls. The earlier cited Anderson Task Force report mentions several of these costs associated with compensating measures:

Higher costs of operation include costs due to separate computers for separate applications, restricting use of remote terminals, costs of physical protection of remote terminals and associated crypto devices, and the costs of clearing all user personnel to the highest level of classified information processed by a system.²³⁰

There is also the cost that derives from the loss of capability or utility. In May 1982 the Director of the NSA made the following statement to a government-sponsored conference on computer security:

For a number of years, computer security (or the lack of it) has had a growing negative impact on our ability to effectively use our computers.²³¹

M. Gen. Robert J. Herres had referred to the same issue when he addressed the 1979 Summer Study on Computer Security:

. . . the way we handle computer security is a barrier to achieving our desired objectives. We don't interconnect and share resources as freely as we would like.²³²

Anderson summarized the problem thus:

The costs of not yet having multilevel secure (MLS) computer systems are inflexible system designs unable to adapt to changes in need, decisions made on incomplete information, and very costly replication of hardware -- all because of the inability to guarantee separation of sensitive from non-sensitive data throughout a computer system.

These problems, serious 12 years ago, are worse today. The inconvenience and security concerns are not limited merely to computers, but today involve whole networks of computers. The "workarounds" involve expensive duplication of networks for security purposes and/or use of extra cryptographic measures for "privacy" within secure networks (i.e., to be²³³ immune to mishandling of sensitive data within switches).

In spite of these real concerns about the costs associated with the lack of sufficiently secure products, industry perceives that there is a definite limit to what even the government's national security sector will be willing to pay. Therefore, industry seems to be making a concerted effort to keep costs within reasonable bounds. Lipner states:

We are exploring what one might do to provide a security kernel that would be at a level of investment consistent with our perception of market value.²³⁴

It often comes down to a tradeoff between cost and security features. More often than not, cost wins. As a former NSA executive points out, the growth in COMSEC was dependent on achieving low cost.²³⁵ Lipner admits that he fears being beaten out on price more than on security features. When asked if he thought some customers would pay an order of magnitude cost premium in order to get security, Lipner replied:

There may be people who would pay it. . . . I guess I would worry that someone else would build a cheaper one [trusted computer] that performed almost as well and knocked the market out from under us before we recovered our investment or developed improved price-performance versions.²³⁶

On the other hand, there are those outside of industry who maintain that, in the long run, cost will not be an issue anyway.

Willis H. Ware, for example, writes:

Society has accepted the cost of providing protection against many threats gradually over at least a century and perhaps longer. In contrast, the whole privacy issue has emerged in less than a decade, and the cost consequences of it have become visible only in the last few years. Thus, in my view, it is the suddenness of the change that is magnifying concerns about cost, and in the long run, I submit that cost will gradually become a non-issue. What society wants, society agrees to pay for.²³⁷

So far, we have examined some of the risks and issues associated with the presence or absence of information security products, in general, and the factors that might influence the availability of such products. But what about separation? What are some of the stakes involved in this question? For example, how might a decision to retain or not retain the current separation affect profits in what might be called the "information security products industry?" Some insight into this last question can be found through a review of the history of what is now known as DoD's Defense Data Network.

The origins of this network can be traced to the Defense Advanced Research Projects Agency (DARPA, or as it was once called, ARPA) Computer network, known as the ARPAnet. During the mid- to late-1960s, ARPA "was supporting numerous large computer installations at various universities and laboratories" engaged in "basic and applied research throughout the U.S."²³⁸ It occurred to people at ARPA that time zone differences meant that different computers were busy or idle at different times, and that by taking advantage of this fact, these computer resources could be shared. Since no appropriate computer networking capability existed at the time, ARPA decided to develop one. With the help of its prime contractor, Bolt, Beranek and Newman (BBN) of Cambridge, Massachusetts, and applying the new technology of packet

switching,²³⁹ ARPA succeeded in developing the ARPAnet, which has since served as the "prototypical packet-switched data network" for the entire world.²⁴⁰

In 1969 the first four nodes of the ARPAnet were installed,²⁴¹ and in 1972 the first public demonstration of the network took place.²⁴² In 1973 both the World Wide Military Command and Control System (WWMCCS) community and elements of the intelligence community began planning data networks patterned after the ARPAnet. The three-node prototype WWMCCS Intercomputer Network (PWIN) and, later, the six-node WIN as well as the Washington-area Community On-Line Intelligence Network (COINS) all made use of the ARPAnet technology. The ARPAnet itself has grown from the original 4 to 95 nodes and over 200 host computers.²⁴³

The success of these packet-switched networks encouraged the DoD to be more ambitious. A 1972 DoD study "projected that by the 1980's there would be approximately 2500 computers and 20,000 input/output terminals in the Defense Community requiring advanced communications facilities." After considering various technical options, the DoD selected packet switching as the most viable technology to meet the requirement.²⁴⁴ DoD called its new program AUTODIN II, after its older record message system, AUTODIN (an acronym standing for "automatic digital network"), which thereafter became known as AUTODIN I.²⁴⁵

Walker writes:

The AUTODIN II program was intended to provide multilevel secure service across all levels of sensitive data (as now provided by the AUTODIN I record message system) from unclassified through Top Secret including compartmented data.²⁴⁶

In 1975 the Director of Telecommunications and Command and Control Systems (DTACCS) approved the AUTODIN II program, permitting the Defense Communications Agency (DCA) to proceed into contract.²⁴⁷

There were two competing teams. The first consisted of Telenet, Northrop Page, and BBN. They proposed a variation of the ARPAnet. The second team was led by Western Union Telegraph Company, supported by Ford Aerospace & Communications Corporation and Computer Sciences Corporation.²⁴⁸ This second team proposed a design based upon security kernel technology.²⁴⁹

The philosophies underlying the two proposals were vastly different. The Western Union proposal involved but four nodes, all to be located at fully cleared facilities and employing large and relatively expensive "trusted" computers. Between nodes, data was to be encrypted, but within the node itself, it would not be. This philosophy of encryption is known as "link encryption." The Telenet proposal was to employ a large number of relatively inexpensive nodes, located at uncleared facilities and employing untrusted computers. In the Telenet scheme, encryption would be performed at the message origin point and a message would not be decrypted until it reached its final destination. This encryption philosophy is known as end-to-end.²⁵⁰ In end-to-end encryption, communities of like-cleared users are maintained and enforced through cryptographic key separation. Thus, the Western Union proposal leaned more on COMPUSEC solutions whereas Telenet's depended more upon COMSEC.

In late 1976 the contract was awarded to the Western Union team "as a tariffed leased service Work began in January 1977 with an Initial Operational Capability (IOC) target of January 1979."²⁵¹

As often happens in large systems procurements, not everything

went according to plan. Stephen T. Walker writes:

Beginning in 1979, the AUTODIN program encountered a number of IOC slips and the other DoD packet switched networks which were intended to be integrated into AUTODIN II continued to evolve. . . . In July 1980, following an IOC slip to December 1980, the Assistant Secretary of Defense for C³I directed a review to identify alternatives to AUTODIN II which would²⁵² be used in case the network should fail to achieve IOC.

Not surprisingly, this review developed only one viable alternative -- a network, based on the ARPAnet and the WIN, that depended upon encryption to provide the requisite multilevel security. Since the system was seen as a "replica" of ARPAnet and WIN, the "new" system proposal came to be known, during the ensuing rematch of the earlier contractual shoot-out, as "REPLICA."

The alternative review determined that, with the right kind of device, some existing nets could be interconnected and expanded. What was needed was a device capable of providing cryptographically-enforced separation across multiple networks and a large range of host computers. Already in use on the ARPAnet was a device, called a Private Line Interface (PLI), to effect cryptographic separation on a single network. Developed during the mid-1970s, the PLI is inserted between a host computer and an ARPA network node. It consists of a cryptographic device sandwiched between two minicomputers. Since the cryptographic device encrypts everything that passes through it, and since the network needs to know what to do with a particular message or packet when it gets it, some way must be found for header information to avoid passing through the encrypter. In the PLI system, the plaintext side of the PLI, often referred to as the "red" side, sends an index number directly to the encrypted or "black" side, bypassing the crypto device. The black side uses the index to look up the

address of the intended recipient of the message and then appends this address to the encrypted message when it releases it to the network.²⁵³

To serve as an alternative to AUTODIN II, something analogous to the PLI but capable of working across networks was needed. A concept was formulated, and in 1980 planning began for the development of a new device to be called the Internetwork Private Line Interface (IPLI). The program, as originally conceived, called for limited deliveries of IPLI devices in 1983 with production quantities becoming available in 1986. The IPLI was key to the whole idea. Its development was seen as the only impediment to making the backup alternative possible.²⁵⁴

Meanwhile, testing of the AUTODIN II system had begun. In the midst of these tests, the projected date of the IOC was delayed again, this time to May 1981. Eventually, during June 1981, system-wide tests were favorably concluded and government security tests were also completed. Walker writes:

On July 6, 1981 the Director of DCA declared limited IOC effective June 30, 1981, and accredited the system for multilevel secure use from unclassified through Top Secret.²⁵⁵

Walker reports that at this point, in spite of the accreditation, there were still two lingering concerns with the AUTODIN II system -- cost and survivability. These concerns, coupled with early favorable indications from the alternatives study, led the Director of DCA, in September 1981, to establish two competing design teams. "One team," according to Walker,

was charged with designing the best possible survivable AUTODIN II system. The other team was charged with designing the best possible alternative system based upon a replica of the ARPAnet and WIN.

In other words, the second team was being asked to design a system

based on the earlier alternatives study. At the same time, the Defense Science Board was asked to establish a task force to examine the same issue.²⁵⁶

Both efforts were given short deadlines so that by early March 1982 the results were in. Based upon the results, both the Director of DCA and the Defense Science Board recommended the REPLICA system.

Then, as Walker reports:

On April 2, 1982, the Deputy Secretary of Defense directed the immediate termination of the AUTODIN II network and the implementation of a Common User Defense Data Network (DDN) as proposed by the Replica team.²⁵⁷

This was a major decision. It amounted to scrapping a multimillion dollar system that worked, despite the concerns that it generated. It also meant paying off Western Union. Termination costs, which would have to be negotiated, would cut into any anticipated cost savings. (Western Union asked for \$21 million in reimbursement for expenses plus \$14 million in contract termination charges.²⁵⁸) It also meant a delay in the realization of a fully operational system. Indeed, the government had a lot at stake in the decision.

Obviously, so did industry. There were clearly very large economic stakes involved in the battle over the right to build the ultimate DDN system. For example, the DCA's estimate was that over the next 10 years the government would pay Western Union a total of \$550 million for AUTODIN II or \$355 million to the BBN group for the REPLICA System.²⁵⁹ Actually, BBN stands to gain from the decision in another way. Originally, the plan was that when the AUTODIN II system was completed, about half of the present set of ARPAnet users would switch to the new network. Now that the AUTODIN II has been cancelled and the realization of a Defense Data Network delayed, it has become necessary

to accelerate improvements to the ARPAnet. One of those improvements calls for the replacement of node computers with BBN's C-30.²⁶⁰

But the victory of the BBN approach over that of Western Union is more than a victory of one company over another. Accompanying the battle for a contract was the battle between the two different approaches. Thus, it represented the victory of one philosophy over another as well. Cryptographic separation won out over trusted computers with kernelized operating systems as the basic approach to isolation in information security systems. A significant point here is that adopting an end-to-end encryption scheme to achieve cryptographic separation did not obviate the need for a trusted computing base (TCB). TCBs are an integral part of any end-to-end encryption scheme. As Walker has written:

. . . security kernels and E^3 [end-to-end encryption] are complementary. There are places where you can not do anything other than with end-to-end encryption. But the critical part of an end-to-end encryption system is a trusted computing base that is included with it²⁶¹

Thus, the difference in the two approaches is not quite as fundamental as it first appeared. Both approaches use TCBs and both employ encryption. The mix is just different. And although security had been one of the principal reasons for building the system in the first place, it was not a major factor in the ultimate decision. Cost and survivability were the dominant considerations.²⁶²

Whether or not the decision to abandon AUTODIN II and embrace the REPLICA was the right one will not be known at least until the new DDN is built. If the REPLICA approach succeeds in yielding a comparable level of security to the AUTODIN II and, at the same time, yields the expected improvement in cost and survivability, it will probably have

been worth the wait. There is little question that the survivability will be improved; the substantial increase in the number of switching nodes virtually guarantees that. But security will be difficult and cost is always uncertain.

With AUTODIN II, Western Union (and the government) learned that security was a much more formidable task than had been anticipated. In fact, Western Union attributes its 2-1/2-year schedule slip to "problems encountered in meeting the security certification standards imposed by Defense."²⁶³

BBN is likely to have some difficulty achieving adequate security on the Defense Data Network also. There appear to be at least three significant security challenges, in addition to countering the subversion threat. To obtain the anticipated degree of security will likely require a secure computer for key distribution, a technical -- as opposed to doctrinal -- solution to the confinement problem, and some clever way to avoid the header bypass problem mentioned earlier.²⁶⁴

The approach now being taken with the Defense Data Network is more modular than that taken by Western Union. Whereas the AUTODIN II employed more of a build-from-scratch methodology, that being pursued by BBN makes more use of existing, "proven" components. Walker, for example, describes the BBN approach as consisting "of an evolution and expansion of existing ARPAnet-technology networks."²⁶⁵ Build-from-scratch systems are generally considered riskier from a cost and functionality point of view but, from a security point of view, are usually preferred. Of particular relevance here is that a more modular approach might well be expected to encounter COMSEC-COMPUSEC

inseparability problems that a build-from-scratch system would not.

Although not associated with security, inseparability problems have already manifested themselves on the ARPAnet. According to a feature article in Data Communications, "when trying to improve throughput and efficiency" on the network, recent experience "has shown that what was thought to be a network or a host problem is actually sometimes a combination of the two."²⁶⁶ Exactly the same thing could happen when BBN goes about trying to solve some of the security problems mentioned above.

Meanwhile, as the DoD waits for a fully operational Defense Data Network, it labors with systems that offer neither the required functionality nor the needed security. The existing threat and latent vulnerabilities suggest that the government -- and, perhaps, business as well -- is already in desperate need of better and more secure products. What is not clear is what will be the government's future strategy for acquiring these products. It is not even clear what the full range of available strategies might be. To explore these questions we need to broaden our list of candidate strategies and to examine more closely the constraints likely to bind the selection. This is important because what now does seem clear is that the choice of strategy may well influence, if not the quality, at least the arrival time of such products.

NOTES for Part III -- The Current Condition

1. Above, pp. II-58, 59.
2. U.S., National Communications Security Committee (NCSC), Computer and Telecommunications Security, Report of the Working Group on Computer Security, July 1981, p. 22.
3. From "National Telecommunications Protection Policy," contained as Appendix B in Greg Lipscomb, Private and Public Defenses Against Soviet Interception of U.S. Telecommunications: Problems and Policy Points, Program on Information Resources Policy, Harvard University, Cambridge, MA, Publication P-79-3, July 1979, p. 62.
4. Interview with former member, Office of Telecommunications Policy (OTP), 16 December 1982. See also ibid., p. 7.
5. Victor C. Walling, Jr., Donn B. Parker, and Charles C. Wood, Impacts of Federal Policy Options for Nonmilitary Cryptography, Research Report 32, SRI International, Menlo Park, California, April 1981, p. v.
6. U.S., NCSC, Security, pp. 78-79.
7. Ibid., p. 1 and ibid., Appendix A.
8. Ibid., p. 1.
9. Ibid., pp. 3, 2.
10. Ibid., pp. 71-73, 81.
11. Ibid., p. 76.
12. Ibid., pp. 48, 51.
13. Ibid., p. 51.
14. Ibid., p. 71.
15. Ibid., p. 81.
16. U.S., General Accounting Office, Federal Information Systems Remain Highly Vulnerable to Fraudulent, Wasteful, Abusive, and Illegal Practices, (MASAD-82-18), 21 April 1982, pp. 2-3.
17. 44 USC 3504.
18. U.S., GAO, Systems Remain Vulnerable, p. 21.
19. Ibid., p. 9.
20. Ibid.

21. Ibid., p. 12.
22. Ibid., p. 18.
23. 44 USC 3901 et seq. and 44 USC 3504.
24. Eugene V. Epperly, "Computer Security Policies: Challenges and Prospects," Proceedings of the Fifth Seminar on the DoD Computer Security Initiative, National Bureau of Standards, Gaithersburg, MD, 24-26 May 1982, p. 110.
25. Lincoln D. Faurer, "DoD Computer Security -- A New Initiative," an address to the IEEE Computer Conference 81, Washington, D.C., 15 September 1981.
26. Interview with Harold J. Podell, Mission Analysis and Systems Acquisition Division, General Accounting Office, 31 August 1982.
27. U.S., GAO, Systems Remain Vulnerable, p. 7.
28. Samantha Fordyce, "Computer Security: A Current Assessment," Computers & Security 1 (January 1982):9, 12.
29. Robert Ellis Smith, "Privacy: Still Threatened," Datamation, August 1982, p. 298.
30. Edwin L. Jacks, "Computer Security Interest in the Private Sector," Proceedings of the Second Seminar on the DoD Computer Security Initiative Program, National Bureau of Standards, Gaithersburg, MD, 15-17 January 1980, p. E-9.
31. Robert Bernhard, "Breaching System Security," IEEE Spectrum, June 1982, p. 24.
32. "A Question of Leadership," Datamation, February 1983, p. 119.
33. Ibid.
34. Ibid.
35. Leslie S. Chalmers, "Panel: The Commercial View of Data Security," 1983 IEEE Symposium on Security and Privacy, Oakland, CA, 26 April 1983.
36. U.S., Congress, House, Committee on Government Operations, Mismanagement of SSA's Computer Systems Threatens Social Security Programs, 97th Cong., 2d sess., 1982, H. Rept. 900, pp. 13, 16.
37. Ibid., pp. 1, 4.
38. Ibid., p. 21.
39. Ibid., p. 22.

40. United Press International, 2 November 1981.
41. U.S., Congress, Mismanagement Threatens Programs, p. 12.
42. Orr Kelly, "Pentagon Computer: How Vulnerable to Spies?", U.S. News & World Report, 31 October 1983, p. 37.
43. Interview with James H. Burrows, Director, Institute for Computer Sciences and Technology, National Bureau of Standards, 1 September 1982.
44. Ibid.
45. Ibid.
46. Above, pp. II-79, 80. See also Appendix A.
47. Interview, Burrows.
48. Interview, Podell.
49. Interview, Burrows.
50. U.S., GAO, Federal Information Systems, p. 24.
51. Ibid.
52. Ibid., p. 28.
53. Ibid., p. 29.
54. Ibid., p. 27.
55. Interview with Peter G. Neumann, Assistant Director, Computer Science Laboratory, SRI International, 25 January 1983. This same problem is also mentioned in U.S., NCSC, Security, p. 81.
56. Faurer, "DoD Computer Security."
57. Ibid.
58. Interview with Col. Roger R. Schell, Deputy Director, DoD Computer Security Evaluation Center, National Security Agency, 28 October 1982.
59. Interview with John P. L. Woodward, Group Leader, Computer and Networking Technology, The MITRE Corporation, 11 August 1982.
60. Telephone interview with James P. Anderson, 18 May 1983.
61. Ibid.
62. Interview, Woodward.

63. Ibid.
64. Interview, Schell.
65. Scherer admits to having had discussions with IBM as well as with other companies. However, according to Scherer's account, the dropping of all references to a security kernel was the less important of two changes he directed. The more important change, in Scherer's view, was a modification of the system acceptance criteria to make it more explicit. Scherer considered the wording of the draft RFP to be too loose to be of much help to the contractor and constituted what Scherer termed "malicious mischief" on the part of the government. (Robert H. Scherer, telephone interview, 28 May 1983).
66. Interview, Schell.
67. Ibid.
68. Ibid.
69. Ibid.
70. Interview, Woodward.
71. Melville H. Klein, "Information Protection Initiatives in the Department of Defense," undated remarks prepared for presentation to the Computer and Business Equipment Manufacturers Association (CBEMA).
72. Faurer, "DoD Computer Security."
73. U.S., DoD Computer Security Center, Trusted Computer System Evaluation Criteria, Draft, 24 May 1982.
74. U.S., Department of Defense, Trusted Computer System Evaluation Criteria, Report CSC-STD-001-83, 15 August 1983, p. v.
75. Ibid., pp. 11-50, 3-5.
76. Interview with Harry B. DeMaio, Director of Data Security Programs, IBM Corporation, 17 August 1984.
77. Lincoln D. Faurer, "Keynote Address," Proceedings of the Fifth Conference on the DoD Computer Security Initiative, National Bureau of Standards, Gaithersburg, MD, 24-26 May 1982, p. 4.
78. U.S., Evaluation Criteria, p. 57.
79. Lester I. Fraim, "Multi-Level Security Today," Proceedings of the Fifth Seminar on the DoD Computer Security Initiative, National Bureau of Standards, Gaithersburg, MD, 24-26 May 1982, pp. 233-240.

The following specific reference to the extent of the performance degradation is taken from the remarks of Rich Neely, as quoted in "Panel Session: Kernel Performance Issues," Proceedings of the 1981 Symposium on Security and Privacy (Los Angeles, CA: IEEE Computer Security Press, 1981), p. 166:

A supervisor (the Emulator) was used to provide the functionality of UNIX, and was built on top of the basic kernel. We ended up with two very complex operating systems, one implementing the other as an interpreter. The result is a factor of ten reduction in performance with respect to UNIX.

80. U.S., National Security Agency, DoD Computer Security Center, "Product Evaluation Bulletin" on the Secure Communications Processor (SCOMP) of Honeywell Information Systems, Inc., Report No. CSC-PB-01-83, 15 April 1983.
81. Interview, Podell.
82. Above, p. III-14.
83. See Zella Ruthberg, "Computer Security Evaluation and Certification," Proceedings of the Fifth Seminar on the DoD Computer Security Initiative, National Bureau of Standards, Gaithersburg, MD, 24-26 May 1982, pp. 207-215.
84. Above, p. II-77.
85. Proceedings of the Seminar on the DoD Computer Security Initiative Program, National Bureau of Standards, Gaithersburg, MD., 17-18 July 1979, p. iii.
86. Ibid.
87. J. Barton DeWolf and Paul A. Szulewski (eds.), Final Report of the 1979 Summer Study on Air Force Computer Security, R-1326, The Charles Stark Draper Laboratory, Inc., Cambridge, MA, October 1979, p. 14.
88. J. P. Anderson, "Accelerating Computer Security Innovations," Proceedings of the 1982 Symposium on Security and Privacy, 26-28 April 1982 (Los Angeles: IEEE Computer Society Press, 1981), p. 95.
89. Peter S. Tasker, "Trusted Computer Systems," Proceedings of the 1981 Symposium on Security and Privacy, 27-29 April 1981 (Los Angeles: IEEE Computer Society Press, 1981), p. 99.
90. Interview with Col. Roger R. Schell, Deputy Director, DoD Computer Security Evaluation Center, National Security Agency, 28 October 1982.
91. Above, p. II-3.

92. See above, p. II-77.
93. Stephen T. Walker, "The Advent of Trusted Computer Operating Systems," AFIPS Conference Proceedings 1980 National Computer Conference, Anaheim, CA, 19-22 May 1980 (Arlington, VA: AFIPS Press, 1980), p. 664.
94. DeWolf and Szulewski, 1979 Summer Study, p. 14.
95. Theodore M. P. Lee, "Processors, Operating Systems and Nearby Peripherals: A Consensus Report," Audit and Evaluation of Computer Security II: System Vulnerabilities and Controls, National Bureau of Standards Special Publication 500-57 (Washington: U.S. Government Printing Office, 1980), p. 8-8.
96. DeWolf and Szulewski, 1979 Summer Study, p. 14.
97. James P. Anderson, Computer Security Technology Planning Study, ESD-TR-73-51, Vol. I, October 1972, p. 31. (Reproduced and distributed by National Technical Information Service, U.S. Dept. of Commerce, as AD-758206.)
98. Based on interview with Steven B. Lipner, Engineering Manager, Security Advanced Development, Digital Equipment Corporation, 3 February 1983.
99. See Note 285, p. II-110.
100. Interview, Anderson.
101. U.S., Evaluation Criteria, p. 57.
102. Walker, "Advent," p. 664.
103. Gerald P. Dinneen, "Computer Security Requirements in the DoD," Proceedings of the Seminar on the DoD Computer Security Initiative Program, National Bureau of Standards, Gaithersburg, MD, 17-18 July 1978, p. A-3.
104. Interview, Neumann.
105. See Croke quotation, p. II-77.
106. Interview with John P. L. Woodward, Group Leader, Computer and Networking Technology, The MITRE Corporation, 11 August 1982.
107. Victor C. Walling, Jr., Donn B. Parker, and Charles C. Wood, Impacts of Federal Policy Options for Nonmilitary Cryptography, Research Report 32, SRI International, Menlo Park, CA, April 1981, pp. 7-8.
108. Below, pp. IV-5, 6.

109. Lincoln D. Faurer, "DoD Computer Security -- A New Initiative," an address presented at the IEEE Computer Conference 81, Washington, D.C., 15 September 1981.
110. John Metelski, "Telecommunications Privacy and the Information Society," Telecommunications Policy 2 (December 1978):329-330.
111. Interview with Roland O. Laine, NSA Retiree, 11 November 1982.
112. During World War II, Bletchley Park was the center of the U.K. cryptanalytic effort, Arlington Hall, the center of the U.S. Army effort, and Washington, D.C., the center of the U.S. Navy effort.
113. Ronald Lewin, The American Magic (New York: Farrar Straus Giroux, 1982), p. 147.
114. Interview, Laine.
115. Willis H. Ware (ed.), Security Controls for Computer Systems, Report of Defense Science Board Task Force on Computer Security, The Rand Corporation Report R609-1, Reissued October 1979, pp. vii, viii, 43.
116. The expression "NP Complete" refers to a class of problems that, although theoretically possible to solve on a finite state machine, or computer, are quite difficult and take a very long time -- perhaps as long as a hundred years. Generally, cryptanalytic problems fall into such a class, and if the time required for a solution is sufficiently long, the cryptographic design is considered strong enough for practical purposes. See Dorothy E. R. Denning, Cryptography and Data Security (Reading, MA: Addison-Wesley Publishing Company, 1982), pp. 31-35.
117. Interview, Schell.
118. Ibid.
119. Roger R. Schell, "Computer Security: The Achilles Heel of the Electronic Air Force?", Air University Review, 30 (January-February 1979):29.
120. Interview, Schell.
121. Interview, Woodward.
122. R. Stockton Gaines and Norman Z. Shapiro, "Some Security Principles and Their Application to Computer Security," Operating Systems Review 12 (July 1978):22.
123. Gerald D. Cole, Design Alternatives for Computer Network Security, National Bureau of Standards Special Publication 500-21, Vol. 1 (Washington, D.C.: U.S. Government Printing Office, 1978), p. 33.

124. Interview, Schell.
125. Philip Alan Myers, "Subversion: The Neglected Aspect of Computer Security," (master's thesis, Naval Postgraduate School, Monterey, CA, June 1980), p. 30.
126. Ibid., p. 10.
127. Interview, Neumann.
128. Ibid.
129. Ibid.
130. Dinneen, "Computer Security Requirements," p. A-4.
131. D. W. Davies, D. L. A. Barber, W. L. Price, and C. M. Solmonides, Computer Networks and Their Protocols (Chichester, England: John Wiley & Sons, 1979), p. 2.
132. Above, pp. II-52, 53.
133. Charles Osolin, "Wired Spies," Atlanta Constitution, 3 April 1977, p.16A.
134. Interview, Schell.
135. System High mode defines a condition in which all users have been cleared for all information resident on a given system but not all are considered to have a need-to-know for all the information. (See U.S., Department of Defense Directive 5200.28, "Security Requirements for Automated Data Processing (ADP) Systems," Change 2, 29 April 1978.)
136. Interview, Schell.
137. Ibid.
138. Peter G. Neumann, Assistant Director, Computer Science Laboratory, SRI International, personal letter, 8 December 1982.
139. A. C. Hinckley and J. Mitchell, Issues in Computer Network Security, ESD-TR-78-167, Electronic Systems Division, AFSC, Hanscom AFB, MA, September 1978, p. 13.
140. See, for example, S. T. Kent, "Network Security: A Top-Down View Shows Problems," Data Communications, June 1978, pp. 57ff.
141. For a complete discussion of the Confinement Problem, see Butler W. Lampson, "A Note on the Confinement Problem," Communications of the ACM, 16 (October 1973):613-615, and Steven B. Lipner, "A Comment on the Confinement Problem," Report MTP-167, The MITRE Corporation, Bedford, MA, November 1975.

142. M. A. Padlipsky, K. J. Biba, and R. B. Neely, "KSOS -- Computer network applications," AFIPS Conference Proceedings 1979 National Computer Conference, (Montvale, NJ: AFIPS Press, 1979), p. 375.
143. Ibid., p. 376.
144. See U.S., DoD, Evaluation Criteria, p. 100.
145. See ibid., p. 73 and Lipner, "Confinement Problem," p. 13.
146. Above, p. II-83.
147. Vinton G. Cerf, "Research Topics in Computer Communication," in Lynn Hopewell et al. (ed.), Computers and Communications: Proceedings of the Federal Communications Commission Planning Conference (Montvale, NJ: AFIPS Press, 1976), pp. 39-40.
148. Rein Turn, Trusted Computer Systems: Needs and Incentives for Use in Government and the Private Sector, The Rand Corporation, Santa Monica, CA, Report R-2811-DR&E, June 1981, p. 17.
149. Ibid.
150. Stephen T. Walker, "Department of Defense Data Network," Signal, October 1982, p. 42.
151. U.S., Department of Defense, Defense Intelligence Agency, "DODIIS Network Security Models," DRS-2600-3026-82, February 1982, p. 2.
152. Above, p. II-79.
153. Bobby R. Inman, "Keynote Address: Computer Security Initiative," Proceedings of the Fourth Seminar on the DoD Computer Security Initiative, National Bureau of Standards, Gaithersburg, MD, 10-12 August 1981, p. B-1.
154. William F. Parham, "KGB Spares No Expense on Eavesdropping in U.S.," Norwich Bulletin, 18 April 1982.
155. Tad Szulc, "To Steal Our Secrets," Parade Magazine, 7 November 1982, pp. 14-15.
156. William Webster, "Military and Industrial Spying," Vital Speeches, 1 April 1982, p. 357.
157. James H. Burrows, "Welcoming Address: Fourth Seminar on the DoD Computer Security Initiative," Proceedings of the Fourth Seminar on the DoD Computer Security Initiative, National Bureau of Standards, Gaithersburg, MD, 10-12 August 1981, p. A-1.
158. U.S., General Accounting Office, Federal Information Systems Remain Highly Vulnerable to Fraudulent, Wasteful, Abusive and Illegal Practices, Report MASAD-82-18, 21 April 1982, p. 5.

159. Ibid., p. 7.
160. U.S., Comptroller General of the United States, Computer Related Crimes in Federal Programs, Report FGMSD-76-27, 27 April 1976.
161. Ibid.
162. Richard P. Kusserow, "Computer-Related Fraud and Abuse in Government Agencies," U.S. Department of Health and Human Services, June 1983, pp. 6-7.
163. Turn, Trusted Computer Systems, p. 35.
164. Marc Leepson, "Computer Crime," Congressional Quarterly, 6 January 1978, p. 3.
165. See Vin McLennon, "Do Soviets control markets through eavesdropping," The Boston Globe, 5 April 1983, p. 40 and B. R. Inman, "Managing Intelligence for Effective Use," Seminar on Command, Control, Communications and Intelligence: Guest Presentations -- Spring 1980, Program on Information Resources Policy, Harvard University, Cambridge, MA, Publication I-80-6, December 1980, pp. 151-152.
166. Interview, Schell.
167. Turn, Trusted Computer Systems, p. 35.
168. Ibid., p. 42.
169. Ibid., pp. 36-41.
170. "The Spreading Danger of Computer Crime," Business Week, 20 April 1981, p. 87.
171. Chalmers, "Panel: The Commercial View."
172. Ibid., p. 86 and Martin Lasden, "Computer Crime," Computer Decisions, June 1981, pp. 104-105.
173. "Spreading Danger," p. 89.
174. A growing number of insurance companies including Lloyds of London (which may have been the first), St. Paul, Chubb, and Shand Morahan now offer computer crime policies. See Louis Nevin, "Lloyd's Offers Coverage for Computer Crime," Associated Press, 15 November 1981, and James D. Blinn, "Data Processing Insurance," Data Security Management (Pennsauken, NJ: Auerbach Publishers Inc., 1982), Chapter 83-03-02, p. 9. Policies differ, but at least one company, Lloyds of London, sells an Electronic and Computer Crime Policy as a rider on its Bankers Blanket Bond coverage, which it sells to large financial institutions. Since many losses were already covered in the basic policy -- employee fraud, for example -- the new offering does not represent a major

increase in coverage. (See Robert P. Abbott, President, EDP Audit Controls, Inc., "Panel: The Commercial View of Data Security," 1983 IEEE Symposium on Security and Privacy, Oakland, CA, 26 April 1983.)

175. See, for example, Donn B. Parker, Crime by Computer (New York: Charles Scribner's Sons, 1976), and Thomas Whiteside, "Annals of Crime: Dead Souls in the Computer," The New Yorker, 22 August 1977, pp. 35-65, and 29 August 1977, pp. 34-64.
176. Gina Kolata, "When criminals turn to computers, is anything safe?," Smithsonian, August 1982, p. 124.
177. Marc Leepson, "Computer Crime," Congressional Quarterly, 6 January 1978, p. 3.
178. "Locking the electronic file cabinet," Business Week, 18 October 1981, p. 124.
179. See Edith Holmes, "Ribicoff Agrees to Delay DP Crime Bill," Computerworld, 20 February 1978, p. 9, and Edith Holmes, "Ribicoff DP Crime Bill Called Valuable Weapon," Computerworld, 24 April 1978, p. 9.
180. Stanley L. Sokolik, "Computer Crime -- Need for Deterrent Legislation," Computer Law Journal 2 (Spring 1980):373.
181. "Rep. Bill Nelson and His Federal DP Crime Bill," Computerworld, 28 March 1983, p. 6.
182. Louise Giovane Becker, Computer Abuse and Misuse: An Assessment of Federal and State Legislative Initiatives, Institute for Defense Analysis, Alexandria, VA, IDA Paper P-1798, December 1984, pp. 32, 39.
183. Ibid., pp. 39-40, C-1 - C-3.
184. See "Action Promised on Crime Bill," Computerworld, 3 May 1982, p. 9, and Joseph D. Hutnyan, "Support Sought For Computer Crime Bill," American Banker, 8 April 1983, p. 3.
185. Ronald Rosenberg, "As technology races on, the law tries to keep up," Boston Globe, 15 March 1983, p. 45.
186. Robert Ellis Smith, "Privacy: Still Threatened," Datamation, September 1982, p. 302.
187. Patricia Keefe, "Harvard Law's Arthur Miller Eyes Consensus on DP Law," Computerworld, 7 March 1983, p. 17.
188. Which statute applies depends upon the type of information involved. For example, credit information is covered by the Fair Credit Reporting Act of 1969; educational records are covered by the Family Educational Rights and Privacy Act of 1974; and bank

transaction records come under the Financial Privacy Act of 1980. See Turn, Trusted Computer Systems, pp. 36-37.

189. At first reading, the Fair Credit Reporting Act appears to define a condition of liability for custodians of credit information. But a more careful reading of the act reveals that the liability sections (1681n and 1681o) create such a liability condition only when some other section of the act is violated. And, except where "malice or intent to injure" is involved, there are no other sections of the act that say that the custodian must protect the information against penetration by a third party. See 15 USC 1681 et seq. and Thorton v. Equifax, Inc., 619 F. 2d 700 (8th Cir. 1980).
190. Keefe, "Miller Eyes Consensus," p. 17.
191. Sokolik, "Computer Crime," p. 374.
192. Wesley R. Iversen, "DES Chips Find a New Niche," Electronics, 17 November 1981, p. 87.
193. J. Michael Nye, "Data Communication: to encrypt or not to encrypt," Industrial Research & Development, March 1982, p. 123.
194. Iversen, "DES Chips," p. 87.
195. Lee M. Paschall, "How Secure Is Satellite Data Transmission?", keynote address to the International Association of Satellite Users Seminar, New York, NY, 9 December 1981.
196. Nye, "Data Communications," p. 124.
197. Ibid.
198. Paschall, "How Secure."
199. James A. Schweitzer, Systems Security Technology Manager, Xerox Corporation, letter to John C. LeGates, dated 12 July 1984.
200. Randi T. Sachs, "Encryption," Administrative Management, February 1982, p. 36.
201. Harry De Maio quoted in Sachs, ibid.
202. For discussion of the DES debate, see above, pp. II-47, 48.
203. J. Michael Nye, "Cryptography Market: Products, Costs, Trends," Telecommunications, April 1982, p. 78.
204. Code of Federal Regulations, Title 22, Sections 121.01, 122.01 and 123.01.
205. Interview, DeMaio.

- 206. It should be noted here that some other countries also control exports of cryptographic equipment.
- 207. Nye, "Cryptography Market," p. 80.
- 208. Above, p. I-6.
- 209. Thomas J. Mitchell, "Cryptography: A commercially viable technology," Telecommunications, October 1981, p. 42.
- 210. Walling et al., Impacts, p. 13.
- 211. Mitchell, "Cryptography," p. 44.
- 212. Eb Klemens, quoted in Sachs, "Encryption," p. 91.
- 213. An Assessment of Civil Sector Uses of Digital Data Encryption, Dept. of Engineering and Public Policy, Dept. of Social Sciences and School of Urban and Public Affairs, Carnegie-Mellon University, Pittsburgh, PA, November 1980, p. 45.
- 214. David Kahn, "The Grand Lines of Cryptology's Development," Computers & Security, November 1982, p. 246.
- 215. Turn, Trusted Computer Systems, p. 46.
- 216. Ibid., p. vii.
- 217. Personal interview with person who asked not to be identified.
- 218. Interview, Neumann.
- 219. Interview, DeMaio.
- 220. Interview, Lipner.
- 221. Ibid.
- 222. Schweitzer, letter to LeGates.
- 223. Interview, Lipner.
- 224. Ibid.
- 225. Theodore M. P. Lee, Manager, Systems Security, Sperry Corporation Computer Systems, personal letter, 2 May 1983.
- 226. Interview with Theodore M. P. Lee, 27 April 1983.
- 227. For a discussion of formal risk assessment, see Robert H. Courtney, Jr., "A Quantitative Approach to Security Risk Assessment," Data Security Management (Pennsauken, NJ: Auerbach Publishers Inc., 1982), Chapter 83-02-02.

228. Ibid., p. 6.
229. Ibid., p. 1.
230. Anderson, Planning Study, p. 4.
231. Lincoln D. Faurer, "Keynote Address," Proceedings of the Fifth Seminar of the DoD Computer Security Initiative, National Bureau of Standards, Gaithersburg, MD, 24-26 May 1982, p. 5.
232. Robert J. Herres, "Overview of Computer Security Requirements," the text of a speech included as Appendix C of J. Barton DeWolf and Paul A. Szulewski (ed.), Final Report of the 1979 Summer Study on Air Force Computer Security, The Charles Stark Draper Laboratories, Cambridge, MA, Report Number R-1326, October 1979, p. 130.
233. Anderson, Accelerating Innovations, p. 91.
234. Interview, Lipner.
235. Rosenblum, letter to Oettinger.
236. Interview, Lipner.
237. Willis H. Ware, "Privacy and Information Technology -- The Years Ahead," Computers and Privacy in the Next Decade, edited by Lance J. Hoffman (New York: Academic Press, 1980), p. 20.
238. Roy D. Rosner, "Packet Switching: Getting the Information Through," Computerworld, 5 April 1982, p. 67f.
239. Packet switching involves the breaking up of a message or stream of data from a computer into short segments, or packets, and sending them separately through the network intermixed with other message packets. The packets are then reassembled in proper order at their respective destinations. The concept of packet switching was invented in the early 1960s by Paul Baran and his associates at the Rand Corporation in Santa Monica, CA. See "A Stampede to Packet Switching," Business Week, 18 December 1978, p. 92G. For a comprehensive treatment, see Roy D. Rosner, Packet Switching: Tomorrow's Communication Today (Belmont, CA: Lifetime Learning Publications, 1982).
240. Rosner, "Getting . . . Through," p. 67f. See also Philip J. Klass, "ARPA Net Aids Command, Control Tests," Aviation Week & Space Technology, 27 September 1976, p. 63.
241. Stephen T. Walker, "Department of Defense Data Network," Signal, October 1982, p. 42.
242. "Packet Switching Proposed 15 Years Ago," Aviation Week & Space Technology, 17 September 1979, p. 62.

243. Walker, "Data Network," p. 44.
244. Isador Lieberman, "Autodin II: advanced telecommunications system," Telecommunications, May 1981, p. 43.
245. Although it took its name from the earlier network, AUTODIN II was not a replacement for AUTODIN I. Each provided some functionality that the other did not. For example, AUTODIN I provides specialized electronic-mail service, which was not designed into AUTODIN II. (See "The Autodin connection," Data Communications, June 1982, p. 97.)
246. Walker, "Data Network," p. 44.
247. Ibid., p. 42.
248. Jack Robertson, "Redialing Autodin-2," Electronic News, 7 December 1981, p. 12.
249. Walker, "Data Network," p. 44.
250. For a discussion of the two philosophies of network encryption, i.e., link and end-to-end, see S. T. Kent, "Network Security: A Top-Down View Shows Problems," Data Communications, June 1978, pp. 57ff.
251. Walker, "Data Network," p. 44.
252. Ibid.
253. Ibid., pp. 42, 44.
- A security question arises from this architectural approach, however. Since some information (nominally that extracted from the header) is passed unencrypted from the red to the black side, how can one be sure that it is only header information that is passed? This concern is often referred to as the header bypass issue.
254. Ibid., p. 44.
255. Ibid., p. 45.
256. Ibid.
257. Ibid.
258. "Spotlight on the Autodin II affair," Data Communications, June 1982, p. 35.
259. Ibid.
260. Joseph F. Haughney, "Anatomy of a packet-switching overhaul," Data Communications, June 1982, pp. 85ff.

261. Stephen T. Walker, "DoD Perspective on Computer Security," Proceedings of the Fifth Seminar on the DoD Computer Security Initiative, National Bureau of Standards, Gaithersburg, MD, 24-26 May 1983, p. 68.
262. See "Spotlight on the Autodin II affair," p. 35 and Brad Schultz, "Pentagon Goes with BBN; Brass Kills Plans to Use Autodin II," Computerworld, 12 April 1982, p. 2.
263. Based on interview of Isadore Lieberman, Western Union's director of application planning for the Autodin II project, as reported in "Spotlight on the Autodin II affair," p. 35.
264. For discussions of key distribution, see above, pp. I-6 and II-48, 49; of confinement, see pp. III-55, 56; and of header bypass, see Note 253. With regard to the confinement, or "covert channel," problem, the DoD appears to have been willing, on many of its systems, to define the problem away -- hence the reference to a "doctrinal solution." According to Lipner, ". . . the Defense Department has apparently measured those [covert channels] and decided, doctrinally, that they can live with whatever bandwidth they came up with." (Lipner interview.)
265. Walker, "Data Network," p. 45.
266. Haughney, "Anatomy," pp. 85ff.

PART IV
LOOKING AHEAD

Chapter 10

A Second Look at Strategies

One conclusion from the information presented in Part III of this is that many information systems of both government and business may be suffering from inadequate security. Among the causes of this condition, as we have seen, is an insufficient supply of information security products. But the existence or non-existence of products reflects, to some extent at least, the policies and strategies of the federal government. If we hope to do anything constructive about the inadequacy of security protection, we probably ought to reexamine these strategies and policies in light of the stakes and perceived stakes of the many players involved.

Chapter 8 pointed out that fundamentally different strategies are being pursued in communications security and in computer security. Two major differences characterize the two current strategies. First, COMPUSEC is being conducted openly, seeking unclassified, generally available products that have been developed, for the most part, in an unclassified environment; COMSEC, on the other hand, is largely conducted in secret, is controlled by the government, and seeks government owned and controlled products developed in a classified environment. Second, in the COMSEC world the government willingly bears the risk of development, whereas in the COMPUSEC world the government seeks to persuade industry to bear the risk itself. Chapter 8 went on to present some of the rationale offered for the two points of view. In this chapter, we look at strategies again, but in a different way.

The two contrasting strategies can be thought of as two squares in a two-by-two decision matrix (see Figure 2).

		In What Environment?	
		Unclassified	Classified
Who Bears the Risk?	Industry	Strategy 1	Strategy 2
	Government	Strategy 3	Strategy 4

Figure 2. Decision Matrix of Strategies Concerning Security Product Development

Chapter 8 dealt only with the two diagonally opposite strategies, denoted in Figure 2 as Strategies 1 and 4. In this chapter we expand our candidate strategy list to encompass those in the two remaining squares as well. We specifically examine the two other theoretically possible strategies, seeking working examples or models of both. The comparative advantages, disadvantages, and inherent limitations of all four candidate strategies are then compared.

The Computer Security Initiative is a clear example of Strategy 1, involving as it does the combination of industry risk taking with an open sharing of information. As was stated in Chapter 8, the government has consciously selected this strategy because it wants reasonably-priced, industry-supported products, but it also wants those products to incorporate the best security features known throughout the COMPUSEC community, and it believes that government sponsorship will not achieve the first objective and a classified environment would thwart the second.

Another example of Strategy 1 is the entire line of DES products for unclassified, non-national security applications. Again, the government wants economical, widely available devices. In this case it also wishes to ease the logistics burden associated with government-supplied devices. It has been willing, for those reduced security requirements, to permit users to purchase approved devices directly, without forcing them to go through some central procuring authority such as the NSA.

One point should be made about Strategy 1. One of the major advantages offered for Strategy 1 is that its unclassified environment permits an open sharing of results to the benefit of all. However, this advantage is rarely fully realized in practice. For competitive reasons, the developing companies themselves restrict the dissemination of research results. Sharing, even with the government, is often tightly controlled by the required signing of non-disclosure agreements. As one observer noted:

This doesn't prevent, but it greatly complicates and slows the . . . diffusion and growth of understanding about how to design information-security systems. In some respects, this type of secrecy is a bigger impediment to progress than government classification. . . .

Strategy 2, involving industry-funded development in a classified environment, is the least common of the four strategies. Nevertheless, a working example involving security products does exist -- the Industrial TEMPEST² Program (ITP). The ITP represents an attempt on the part of the U.S. government to ensure an adequate supply of TEMPEST-suppressed word processors, computer terminals, and the like, without paying for their development or having to endure the long waiting time associated with government-funded development. This might

have been easily achieved were it not for a second objective: to retain a measure of control over the more sensitive aspects of the TEMPEST business. The U.S. government did not wish to educate the world. It wished only to educate a small but sufficient number of companies that might be willing and able to produce equipment for the government's own use.

The government fixed upon Strategy 2 for very pragmatic reasons. First, it desired many sources for like products. It wanted diverse functionality as well as competition-driven economy. At the same time, it wanted adequate protection, according to its own definition of "adequate." The government saw no way of obtaining such protection without sharing with the vendor the government's own vision of what constituted adequate security and how to achieve it. No supplier was likely to try very hard to meet a set of technical objectives without being told what those objectives were. It would be too easy for his company to find itself in an endless loop of government testing and government-dictated enhancements. This would be fine with the supplier if the government were underwriting the cost of development -- in other words, pursuing Strategy 4. But the government could not afford to underwrite development at several companies at once, and the whole idea was to involve as many suppliers as possible. Therefore, it was clear that the government would have to share some of its inside information with the vendors.

The rub here was that some of the information that had to be shared was classified. Not only that, but there seemed to be good reasons for keeping it classified. If the government were going to have to give up something, it wanted to be sure that it gained

something. In particular, it wanted to be sure that any company to which it released the classified information made use of that information to build an actual product. Also, of course, it wanted to be sure that the company adhered to all of the standard rules established for handling classified information.

Thus, the ITP was born. The announced purpose of the ITP is "to support U.S. manufacturers who wish to produce TEMPEST-suppressed equipment to sell to the U.S. Government." Access to the government market is provided by means of a Preferred Products List (PPL). The inclusion of a specific product on the PPL indicates to government purchasers that the product meets the "current national standard."³

Strategy 3, although not uncommon in general, does not represent a standard method by which the government acquires security products. However, there is at least one notable case in which this strategy was pursued by the National Security Agency in order to obtain its highest priority need at the time -- although not a security product. The program began in July 1956 at a cocktail party and has been described by Samuel S. Snyder as "one of the most costly as well as far-reaching research programs ever undertaken by NSA."⁴ The name of the program was LIGHTNING.

At this historic cocktail party, according to Snyder's account, were NSA's Director, Lt. Gen. Ralph J. Canine, and "several high-level NSA equipment planners." They were discussing one of NSA's perennial problems -- "the race between analysts' insatiable requirements for new ways to attack always increasing volumes of data and engineers' efforts to design and build bigger and faster computers to meet those needs." The engineers' achievements were always outpaced by the

analysts' requirements. A new computer system, called HARVEST, was under development at the time, but its scheduled completion was still several years away. When Canine was confronted with the problem, he is said to have retorted, "Dammit, I want you fellows to get the jump on those guys! Build me a thousand megacycle machine! I'll get the money!"⁵

Get the money he did. Canine proved as good as his word. Snyder recounts:

The LIGHTNING project received approval of the Deputy Defense Secretary in October 1956, and was endorsed at the Presidential level in a White House conference in December 1956, by Dr. James Killian, with President Eisenhower's backing. Actual work by several contractors was under way in June 1957, the start of a projected five-year program with a funding level of approximately \$5 million per year.⁶

In addition to the substantial government subsidy, the program was guided by the principle that "results of the research would be reported in the open literature and made freely available."⁷ Thus, with the government bearing the risk and in an open unclassified environment, Project LIGHTNING clearly represented the selection of Strategy 3 on the part of the government.

Another more current example of Strategy 3 is the government's Very High Speed Integrated Circuit (VHSIC) Program. Although some aspects of this program have now been classified,⁸ causing it to look more and more like Strategy 4, it was purely an open, unclassified venture when it began and therefore a clear example of Strategy 3.

The VHSIC Program, launched by the DoD in fiscal year 1979 as a six-year program, was aimed at overcoming what was then perceived as a rapid eroding of America's leadership in integrated circuit technology.

Intelligence estimates at the time indicated that the U.S. technology lead had slipped from between 5 and 10 years to between 3 and 5 years and was continuing to diminish. The goal of the program was to so advance the technology of integrated circuits that manufacturers would be able to deliver circuits in production quantities -- not just laboratory prototypes -- that would provide 100 times the processing throughput of then current ICs.⁹ The intent was not to change the direction or the destination, which the manufacturers would have selected anyway, but only to advance the estimated time of arrival.¹⁰ A stated objective from the beginning was that "results of the supporting technology work be made available to all VHSIC primes equally."¹¹ Even companies that did not participate in the program were to be provided with some of its results.¹²

While most integrated circuit manufacturers "vied intensely" to get a chunk of the government's money, two companies -- Intel Corp. and RCA -- spurned the DoD's offer. According to one trade publication:

Intel officials felt VHSIC would divert scarce resources and capital to VLSI [Very Large Scale Integration] work keyed for a more-narrow military market, arguing that DoD should work with industry to adapt evolving commercial VLSI devices to military programs.

As it turned out, there were nine contenders for contract awards -- including single companies and teams of companies -- of which six were awarded contracts, with each of the three services managing two companies.¹³

Strategy 4 is the dominant government COMSEC strategy. In fact, as Chapter 4 points out, from about 1945 until 1977 it was the only government COMSEC strategy. Strategy 4 made sense because it supports a policy of government control better than any other, and, for both

offensive and defensive reasons, government policymakers have apparently believed that such a strategy was in the government's best interests.

So we have four discrete strategies and at least one instance of each one. These examples offer an opportunity to evaluate the four disparate strategies -- to ask, "How have they done? To what extent have the various strategies succeeded or failed?"

One might conclude that the Computer Security Initiative, our example of Strategy 1, has not fared very well. This certainly seems to be the judgment of James P. Anderson, who chaired the Air Force sponsored Computer Security Technology Planning Study in 1972.¹⁴ At a symposium in April 1982 he said:

After nearly twelve years of serious work on computer security, all that can be shown is two one-shot "brassboard" systems and one commercially supported product that integrates the DoD security policy into the operating system.¹⁵

"Twelve years of serious work" would date the beginning of such work as approximately 1970. This was about when the MULTICS work began and a couple of years after the start of the ADEPT-50 project.¹⁶ The fact that the Computer Security Initiative was not launched until 1978 is misleading; 1978 was simply the year that the government decided to announce its strategy publicly and bestow on it some kind of official status. In actual fact, the DoD had already been pursuing the strategy for many years.

Nevertheless, the Anderson judgment may be slightly unfair. After all, building trusted computer systems is not a simple matter. Clearly, it takes time. Also, until very recently industry had no clear statement of what the government standard would be. Industry can

hardly be blamed for not wishing to shoot at what might prove to be a moving target. Finally, as the government learned with its Industrial TEMPEST Program, the first product is always the hardest to get. Once the first product exists and some measurable portion of the government's business gravitates towards it, market pressures take over providing the motivation for other vendors to offer like products. Significantly, this threshold has now been crossed. On 23 July 1984 the DoD Computer Security Evaluation Center completed its evaluation of the IBM product known as "RACF." It was given a "C1" rating. The RACF thus became the first product to be listed on the Evaluated Products List (EPL).¹⁷ Several additional products from a number of vendors are undergoing evaluation. So, although slow to yield results, Strategy 1 may yet prove to be at least a limited success.

The Industrial TEMPEST Program, our example of Strategy 2, clearly represents a far less ambitious undertaking than does the Computer Security Initiative. Still, when it was launched, its success was far from certain. According to an official NSA source, two fundamental assumptions underlay its establishment. The first is that companies know the government market better than the government does, and the second is that the government's best approach in this situation is to tell industry what it wants and then leave industry alone. If the market is truly there, the products will come.¹⁸

This philosophy seems to have worked. Since its tentative beginnings in the mid 1970s, the ITP's growth has been impressive. When officially announced in 1976, it had nine member companies. The first edition of the Preferred Products List (PPL), published in 1979, included 11 products. By the end of 1982 the ITP had grown to 80

members and the PPL listed 84 TEMPEST-approved products.¹⁹ Pointing to this "continued growth in the number of participants," the NSA source states, "I can only conjecture that the people in [the program] are making money The number of dropouts have been few and far between."²⁰

However, the ITP's success must be measured in terms other than mere numbers of members or items on a product list. The ITP could only be judged a success if it had the desired effect upon government procurements. According to the same NSA source, it is now commonplace for government procurements to require that certain classes of products meet the current TEMPEST standard. Although a product could meet the standard without appearing on the list, the reverse is not true. Appearance on the list is prima facie evidence that the equipment meets the standard. Thus, it is common practice, particularly among agencies with limited technical competence in the TEMPEST field, to select products from the list. The NSA source states that the member companies now strive to get a new product on the list at the same time they announce it. He points with pride to the fact that "the list was there and waiting when the world woke up to word processing." Regarding cost, he comments, "I think the biggest thing it does is offer competition." Although admitting that "we don't have a free competitive market," he is quick to add that "some of the costs would be extremely greater if the list were not there."²¹

Thus, when measured against what the government hoped to gain from the ITP when it began the program, the ITP must be judged highly successful. Albeit a small program²² in a relatively esoteric field, the ITP does provide some evidence that Strategy 2 can work.

By most accounts, Project LIGHTNING, one of our examples of Strategy 3, can also be viewed as a success. During its five-year existence it produced 320 patent applications, 71 university theses, and 160 published articles in recognized technical journals.²³ Some of its results were directly applied to special-purpose computer hardware being built for the DoD. For example, while working on one DoD project, relates Snyder:

IBM was confronted with the need for a faster diode in the high-speed memory address-selection matrix. Under LIGHTNING sponsorship, Sperry Rand's Norwalk plant developed a silicon high-conductance avalanche diode that satisfied the IBM requirement.²⁴

Project LIGHTNING proved beneficial to the participating companies as well. Some of the technological innovations developed under LIGHTNING found their way into commercial products. The Univac Model 1107, for example, made use of thin film techniques that had been developed under the program.²⁵

In an overall sense, as James Bamford has written, "Lightning . . . helped prime the scientific pump."²⁶ It helped to speed the arrival of technological developments in high speed computing, which, after all, was precisely what it had been set up to do.

With regard to the VHSIC Program, our other instance of Strategy 3, it is probably too early to judge its success. Besides, since a portion of the program is now being pursued on a classified basis, it no longer constitutes a pure example of the strategy. What it does provide, however, is an example of what can happen when there is a shift, or even a threatened shift, from an open or unclassified to a restricted or classified strategy. Such a shift certainly precipitates quick and strong reaction from academic circles. In the words of

Technology Review, MIT's magazine:

[W]hen the DoD attempted to restrict the publication of unclassified research in this [the VHSIC] area, and the Department of Commerce barred a foreign professor from participating in VHSIC research²⁷ at Cornell, the academic community responded with alarm.

This response suggests a strong stake on the part of the academic community in keeping research unclassified. Their instinctive reluctance to involve themselves in classified research is due, in part, to strong incentives within academe to publish; in part, to practical difficulties in involving graduate students in the research -- particularly those who are foreign or otherwise unclearable; and, in part, to a philosophical conviction that, since research tends to be cumulative, openness produces more synergy and thus better, or at least quicker, results.²⁸

Strategy 4 has had many years in which to prove its value in communications security. From 1945, when the Armed Forces Security Agency made the conscious decision to establish its own cryptomathematics research organization for COMSEC,²⁹ until 1977, there was virtually no other way in which cryptographic devices were developed and produced for government use. And, since 1977, this still constitutes the government's sole strategy for the most sensitive applications.

Over the years, as earlier chapters have described, this strategy has succeeded in yielding a wide range of equipment for widely varying applications. It has not been particularly successful, however, in producing equipment capable of satisfying the needs of either the civil agencies or the commercial market. Of course, it has not been trying to satisfy such needs. Because of the rather unrestricted environments

in which devices for this market must operate, the devices themselves must be unclassified even if the environment to produce them was not.

Although the establishment of NTIA's Special Project Office³⁰ clearly had been strongly motivated by strong political factors, some still believe that it might never have occurred if the NSA were already responding adequately to the needs of the civil agencies. NSA would have been willing to sell its classified cryptographic equipments to the civil agencies, but the civil agencies were not at all eager to buy them. Since the equipments were "special order" devices (a direct result of government sponsorship), they tended to be expensive. And their classified status imposed constraints on their handling that the civil agencies were not prepared to accept. Thus, in 1977 there existed a void and NTIA was chosen to fill it. The fact that NTIA is no longer doing so is beside the point. Of much greater significance is the fact that the need is now being met, but through the pursuit of a different strategy -- Strategy 1. In general, the requirements of the civil agencies are being satisfied through industry-developed equipment -- most embodying the DES³¹ algorithm. Strategy 4 had not been up to the task.

These experiences show that different strategies succeed at different things. Indeed, each of the four strategies seems to have advantages as well as limitations. Which of the four is the most appropriate for a particular security product may depend partly on the degree of protection or assurance required. There would appear to be some correlation between the chosen strategy and the amount of confidence one can prudently place in a given product. Thus, the selection of a particular strategy may impose limits on the environment

or on the range of applications in which one might feel safe using the product.

The government believes that it takes a greater security risk when it accepts a commercial product designed and assembled in a relatively uncontrolled environment. Because of the risk of subversion, this is true even if the product is fundamentally more robust than what the government could or would have developed on its own. However, there are many environments and applications for which this risk is quite acceptable and for which it would probably be senseless for the government to assume the greater cost or accept the longer delay inherent in government-sponsored, classified developments. The government must find a way to assure itself that the risk it is taking in a given application is and will remain prudent, without having to invest an inordinate amount of time analyzing the environment, the product, or both.

A classified environment, on the other hand, imposes some measure of additional control. Specifically, it limits the physical access to classified portions of the hardware and software only to persons holding the appropriate clearance. Classification also establishes rules for storing, transporting, and accounting, which should reduce the risk of tampering or of subversion. The absence of these controls tends to establish an upper bound on the amount of trust a given system can prudently be given. According to Schell,

. . . if I'm going to use commercial unclassified developments . . . as a base, there's a set of things that I can no longer do anything about. . . . I believe that the technology . . . [allows us to] assume a sufficient set of conditions for correct design of hardware . . . but we are not going to be able to take [a] chip and answer the question where it's [been]. I'm going to have to have control, or at least visibility . . . over where that chip

came from. And so, I'm relatively pessimistic [regarding] our ability to take commercial products in the long term -- say . . . a 20-year time span . . . -- and use them for highly secure applications where I really care.

When asked how he would deal with this problem, Schell replied:

From my point of view, I know only one way to do it. That is, I will have to bring that development under a classified control system I have to have visibility. I have to know where it [the hardware] came from and how it got there.

Thus, Schell foresees a need for the computer security community eventually to adopt a different strategy. While supporting the Computer Security Initiative "as the proper direction for the time and place," Schell states, "We'd better be ready to add a new component to the strategy in ten years."³²

In addition to controlling the environment, a classified or secret strategy has the advantage of retarding the transfer of the applicable technology to any potential adversary. This is highly advantageous in the ongoing battle over information among nations. It makes little difference how strong a country's offensive or defensive capability is if its opponent's capability is as good or better. For convincing evidence of this principle, we need look no further than the Second World War.

During World War II, the fortunes of the shooting war seemed to be closely linked to the fortunes of the information war -- particularly in the European theater. The turning point of both is usually given as sometime in early 1943 when the Allies turned their full attention to gaining control of the Atlantic by defeating the U-boat threat.³³ They were able to do this by exploiting their cryptologic advantage. Don E. Gordon writes:

The allies won WW II by finally multiplying the combat power of existing resources and destroying the resources of the enemy. The allies did not learn how to do this quickly; it took until mid-1943, and required³⁴ that intelligence be considered as a strategic objective.

Just as the military advantage initially lay with the Axis powers, so did the cryptologic,³⁵ and with it, the information advantage. Patrick Beesley writes:

. . . if, by the third year of the war, the British were beginning to have a distinct advantage -- not only in the field of cryptanalysis but in all other areas of operational intelligence, it is certainly³⁶ true that in 1940 the boot was very much on the other foot.

The cryptologic advantage proved to be extremely important -- so important, in fact, that many historians now place it among the decisive factors in the outcome of the war. And, according to F. W. Winterbotham, author of The Ultra Secret, this was also the judgment of Eisenhower.³⁷ But what aspect of cryptology provided the edge? Was it the absolute strength of the Allied cryptanalytic effort? No, because if the cryptography of the Axis powers had been stronger, our cryptanalysis would not have been as successful. Was it therefore the superiority of our offensive measures over their defense? The answer to this must also be, "No," because if their offense had been equally superior to our defense, any advantage accruing to our side would have been neutralized. In particular, as was pointed out in Chapter 8,³⁸ they would have learned the extent of our cryptanalytic success and would surely have changed their cryptographic system -- just as we changed one of ours under reverse circumstances. In January 1943, when the U.S. Navy learned from ULTRA that the Germans were reading the Allied Combined Convoy Code, the Navy developed a more secure code and replaced the original.³⁹

While our offense was attacking their defense, their offense was attacking our defense as well. What proved decisive in this engagement was a net team advantage -- our offense over their defense as well as our defense over their offense. As Gordon writes:

World War II was fought to a decisive conclusion largely because of the impact of electro-mechanical encipherment and cryptanalysis devices, radio direction finding radar, and counter radar devices [emphasis added].⁴⁰

There is nothing surprising or profound here. Such a net team advantage is what generally decides all forms of conflict whether they be friendly parlor games, team sporting contests, or wars. And, just as in other forms of conflict, secrecy contributes to any net team advantage.

On the other hand, sharing of information can also be useful. An unclassified or open strategy has the advantage (particularly when the technology is new or when the government lacks a monopoly on available talent) that whatever is being developed can incorporate the best and most creative ideas from virtually all sources. Particularly when one of the desired sources is academe, an open or unclassified strategy will almost always be more successful in ferreting out the academic input. (In fact, some universities will not accept any classified research at all.⁴¹) Advocates of an open environment point out that not only can the initial design profit from this broader input, but the analysis or evaluation of the proposed design is also likely to benefit. As George I. Davida, a university researcher in cryptography, wrote, "Clearly the field often benefits from the independent viewpoints of academic researchers -- not only as inventors, but as constructive critics as well."⁴² By publicizing the proposed design, say the openness proponents, it is far more likely to be subjected to

analysis and evaluation by a much wider community and therefore any inherent flaws are more likely to be uncovered before the design is finalized. As another independent researcher points out, "If . . . a system is made public it will be subject to scrutiny by a wide range of critics and weaknesses are less likely to be overlooked."⁴³

An open strategy also has the advantage that it tends to be cheaper. For all their attendant benefits, security and classification cost money -- often a great deal. The value of classification may not be worth its cost.

The value of classification or secrecy seems to be related to the strength of the mechanism it protects. As Neumann points out, classification makes sense only if the security strength is neither too strong nor too weak. Under these circumstances, says Neumann, the classification process can buy time, which may be all it needs to do.

Speaking from a computer security point of view, Neumann states:

At one end, the flaws are so obvious that any moron can find them. Classification does not help you at all The other extreme is where the system really is tremendously secure (which has never happened before) -- where all the proofs go through and everything is really clean. In that case, classifying is again silly But, in the middle, there is the case where knowledge of the specs or of the proofs . . . can really gain some information.

So, whereas in principle, I believe that everything should be open, I think there are times when you have to keep some distance in time between you and your pursuers -- in which case classification acts as a delaying mechanism. It's sort of like a crypto key where it might take the guy two years to find it, but, by then, you've changed the key.⁴⁴

Since most well-designed systems fall well away from the two extremes, Neumann's argument tends to support classification.

However, as Neumann also points out, two practical questions arise when the government sets out to implement a strategy of secrecy: where

does the government draw the line and how useful is the classification once the line is drawn? Neumann argues:

Now the argument has been used that you have to classify the [results of] penetrations and the counterpenetrations and the proofs because if you didn't, then clearly people could penetrate the system Well, if anybody had the specs and the code, they could regenerate the proofs assuming the proof tools are in the private domain. (The specs are in the private domain and the proofs are in the public domain.) So, if you're going to classify the results of the proofs, then you'd better classify the proofs and the code and the specs. . . . Where do you stop?

Now, if you don't classify the specs, for example, but you do classify the code, then nobody can regenerate the proofs. On the other hand, it's pretty hard to maintain the system. . . . Now, you can classify the tools that you used to do the proofs. That gets pretty stupid because you want those to be widely used by industry.

So there are some very funny problems here in inference. No matter what pieces you have, you can infer something else.⁴⁵

For a security policy to be helpful, it has to be consistent; and for it to be respected and observed, it must be viewed as reasonable. As Neumann's argument shows, these are often in conflict.

Turning to the other dimension on our matrix, we note both advantages and disadvantages of government sponsorship or risk-taking. Government sponsorship has the advantage -- at least to the government -- of allowing the government access (and legal rights) to virtually all of the design details. Since the government bought and paid for the design, it owns it. When industry develops a device or system on its own, it may or may not be willing to reveal even all of the security-relevant details. This surely increases the government's risk.

One way to compensate for this disadvantage is through some form of government certification such as the ITP's Preferred Products List or the Evaluated Products List of the Computer Security Initiative.

Under the rules established for these lists, if a company wishes one of its products to appear on the list, it must make available to the government sufficient information on which to base a security judgment. Of course, the listing is voluntary but if a producing company is unwilling to share this information with the government, the product does not receive the government's certification and a certain slice of the market is foregone.

Industry sponsorship offers the advantages of economy and support. If industry develops the mechanism, it does so with a broad market in mind. A broad market usually yields lower prices due to both the economies of scale and the competition that a large market generally attracts.

Support is a slightly more elusive concept, yet can be a most important consideration. It implies, first of all, some willingness on the part of the vendor to stand behind his product -- something of the notion of a warranty. It implies, too, the ready availability of professional maintenance and service. And it implies compatibility with other products. When applied to a secure operating system, for example, "support" means that the operating system can accommodate some of the more useful applications software that is available. As Anderson puts it, "I want a system that runs interesting things." He says he does not want what he calls a "special product" or a "one shot," and offers the Kernelized Virtual Machine (KVM) as an example of such a special product.⁴⁶ The KVM was a government-supported project at the Systems Development Corporation, now part of the Burroughs Corporation, to develop a secure operating system for the IBM-370 computer.⁴⁷

Since each of the four strategies has its own set of attendant advantages, we might expect to find individual proponents for all four. This appears to be true. Anderson, whose criticism of Strategy 1 for computer security has already been recounted, is an advocate of a modified Strategy 3. William P. King, a retired COMSEC developer, supports a modified Strategy 2. And the arguments offered in support of Strategies 1 and 4 were set forth in Chapter 8.

One's strategy preference is likely to be largely determined by what one believes the government should be attempting to do. Should the government be trying to satisfy all of its information security requirements by attempting to get developed mechanisms that are robust enough for all environments? Or should it be striving, as a first step, to simply improve the security in all environments and, in the process, to achieve a level of protection adequate for some of them? In his answer to these questions, Schell favors improvement:

The view which I happen to subscribe to . . . says our real objective ought to be to improve security, not to achieve security. I think that there are really dramatic improvements in security that we can make.⁴⁸

This is not a simple issue. If the government concentrates only on improvement, it is almost surely delaying the arrival of the adequate. But should the government devote all of its attention to the development of the adequate, such development is likely to take considerable time and, meanwhile, leaves all information inadequately protected.

It appears to be a matter of risk. Many people fear that if the government aims too high, it might get nothing. They are concerned that by requiring or demanding too much in the way of security, the

government may scare away all potential suppliers. To a joint gathering of government and industry people, Walker stated:

You may accuse me of advocating a less than perfect solution Far from that, though, I am advocating seeking a reasonable, useful solution prior to seeking the perfect solution. Indeed if we do not make serious attempts to crawl before we run here, we very likely will never get anywhere near that perfect solution.

According to Walker, most environments do not require "that perfect solution," anyway:

not very many applications require a system to operate over anything like the full range of sensitive information
. . . many of our security requirements can be met by systems that operate over a limited range of new line sensitivity

However, a most important implication of Walker's statement is that there are some applications that do require near-perfect security.

Of course, the government need not worry so much about scaring suppliers away if it is willing to at least share some of the cost of development. This would appear to be the opinion of Anderson. In his advocacy of what is here called Strategy 3, Anderson alludes to both the VHSIC and the LIGHTNING programs:

Since the manufacturers are unwilling or unable to develop secure systems on their own, it is proposed that the development be underwritten by the federal government in a way that rewards those manufacturers who have spent the most in R&D or security in a way that will benefit their product line systems.

As a model for the type of support proposed, it is suggested that the DoD's VHSIC program be considered. An older example of government underwriting needed technology is found in the Lightning program of the late 1950's.⁵⁰

Although conceding differences between COMPUSEC and high speed circuitry, the goal of both the VHSIC and LIGHTNING programs, Anderson justifies his recommendation:

While the VHSIC program is not exactly comparable to the need for secure computers for national security applications, it does form a model that demonstrates that the government is able to fund R&D and prototype work among a number of competing manufacturers in order to achieve a particular technology and products needed for national defense purposes.

In spite of the above statements, Anderson actually does not favor the strict pursuit of Strategy 3. In an interview Anderson explains that, although he favors retaining much of the spirit of Strategy 3, what he favors is more like Strategy 4 -- at least for some of the more demanding environments. Says Anderson: "If I were doing it, I would do it with the government sponsoring the work, in a classified environment." Anderson readily admits that it is the threat of subversion that most concerns him, stating: "I worry about subversion. I worry about subversion all along the line -- not just during development." At the same time, Anderson wants the product that emerges from the protected environment to be unclassified (as are most TEMPEST products).⁵² Anderson is convinced that only if the security features are part of a vendor's product line -- and thus supported and maintained -- will they be useful.⁵³ But for a product to be part of a vendor's main line it must be unclassified. Hence, Anderson's strategy represents something of a compromise. Whether or not it is a good compromise may hinge on whether the cost savings deriving from the economies of scale that a main line product ought to enjoy will be sufficient to offset the added costs of the protected environment.

Retired NSA engineer William P. King, who spent his entire career working in the COMSEC R&D organization, advocates a modified Strategy 2. He suggests a process

. . . whereby industry would develop a security component such as a module, VHSIC chip, etc. in a classified

environment but with the end product being an unclassified but controlled and verified⁵⁴ item which could be incorporated into manufactured systems.

Presumably, the design for King's module would be supplied by the government.

Although such a strategy might prove advantageous in COMSEC development, it is not clear that it would yet be helpful as a way of producing COMPUSEC products. Strategy 2 appears to offer an advantage only when the government has some proprietary knowledge, protected by classification, that a product requires in order to be sufficiently robust. This seems to be true in COMSEC. But in computer security and in information security, it does not appear to be true. Rather, it appears that all involved are still groping for solutions. No one, including the government, yet has a monopoly on the innovative ideas necessary to "solve" the information security problem. Thus, Strategy 2 does not emerge as the most promising since it would have the effect of foreclosing the collective search for solutions that is taking place now.

Also, in COMPUSEC there is evidence of a predisposition to the belief that Strategy 2 will not work. Former NSA Director Inman, for example, has stated:

The [DoD Computer Security Evaluation] Center will have a difficult task developing procedures which assure protection of sensitive portions of a system which the government does not own. Simply classifying security related portions of a system built by industry won't work since the government represents such a small portion of the overall market that the manufacturers may well decide not to sell to the government rather than accepting the limitations imposed by classification.⁵⁵

With respect to the other three strategies, each has its own attendant advantages, and choosing one over the others would be

difficult. But perhaps it is also unnecessary. It may be possible to accrue the advantages of different strategies simply by pursuing more than one at a time. There is nothing mutually exclusive about these strategies. Apart from the ever-present resource constraint, the pursuit of one does not have to inhibit the pursuit of another. The COMSEC world seems to have hit upon a mixed strategy to satisfy the diverse needs of both the government's national security and the civil sectors. In computer security there certainly seems to be room for the strategy of the Computer Security Initiative (Strategy 1), but there may be need for another as well -- one that offers increased protection against the subversion threat, perhaps something closer to Strategy 4. Pursuing different strategies in parallel seems preferable to pursuing them sequentially, as Walker appears to be suggesting.⁵⁶

Beyond computer security, in that hard-to-pin-down world of information security, there is probably good reason for the government to actively pursue more than one strategy as well. It is always dangerous to put all of one's eggs in a single basket. The basket might break or it may prove too small to accommodate all the eggs one finds he needs. Better to accumulate several baskets.

In addition to pursuing different strategies on different systems at the same time, it is also possible to pursue different strategies at different times. Strategies could vary during different stages in the system's life cycle. For example, one might wish to classify a system during design but to declassify it when it enters production. Or the government may wish to help fund exploratory development to the point of establishing feasibility, and then to back off and allow market

pressures to take over. In fact, this was the basic philosophy behind the Air Force COMPUSEC program in the mid-1970s.⁵⁷

Finally, we return to the issue of separation. As part of their overall strategy, should the government, industry, and business be jointly striving to eliminate the technologically artificial distinction between COMSEC and COMPUSEC? In one respect, at least, separation may not be an "issue" at all. If we use history as our window into the future, we would likely conclude that, sooner or later, the separation between COMSEC and COMPUSEC that we see today will gradually disappear. Within the NSA, for example, Inman predicted that "in four or five years" an organizational integration was entirely possible. He did, however, offer one important qualification:

I would think, over time, if this process really works -- if the computer security center at NSA really produces success -- that it would be entirely feasible for the computer center and the COMSEC organization to become a single organization.

But he added that he believed that "it will come about only after there has been substantial success."⁵⁸ Presumably, in addition to a set of technical and administrative achievements, "substantial success" would imply reasonable size and strength to avoid the risk of subjugation (discussed in Chapter 8) when the COMSEC and COMPUSEC organizations are combined.⁵⁹

Industry, too, is apt to witness this inevitable evolution toward further integration of the two technical problems. As industry grapples more and more with network security problems, it will very likely be forced to think increasingly in information security terms. As James J. Croke, Vice President, Bedford Operations, of the MITRE Corporation points out:

[W]here encryption-enforced protection needs to work closely with protection on a smaller granularity (e.g., individual transactions between [trusted] computers), there is a need for integration of the traditional communities, with those contractors best able to address⁶⁰ the problem leading (forcing) the integration of the two worlds.

In fact, there is some evidence that this melding has already begun. One major company, at least, has already taken steps to integrate its COMSEC and COMPUSEC activities. In December 1980 the Burroughs Corporation acquired majority ownership of the System Development Corporation (SDC). As has already been recounted in Part II, Burroughs had long been active in communications security while SDC had been involved in computer security at least since 1966. Less than two years after the acquisition, on 12 August 1982, Burroughs Chairman and Chief Executive Officer W. Michael Blumenthal announced the merger of the Burroughs Federal and Special Systems Group (that part of Burroughs involved in COMSEC) with the SDC. The new organization was named "Systems Development Corporation, A Burroughs Company."⁶¹ It is too early to assess either the effect or the effectiveness of this merger. In fact, geography is likely to inhibit, or at least retard, the full realization of Chairman Blumenthal's intent since the Federal and Special Systems Group is located in Paoli, Pennsylvania, while SDC headquarters are in Santa Monica, California. Still, the Burroughs move is interesting and may be a harbinger of similar actions by other companies.

Such a convergence of the two problems may influence strategy. It seems reasonable to expect that as we separate less, we will have to classify more. Whereas it may well be possible to keep unclassified a single feature embodied in a single component product, when many features are combined interdependently into a more complex product, it

becomes increasingly difficult to avoid classification. The more that is included within a given system, the higher the stakes rise and the greater the pressure (and need) to protect that system through classification.

Success and progress, then, appear destined to drive the government to include at least a classified component in its bag of assorted strategies. Since it is probably premature to abandon Strategy 1, it may be time for the government to enrich its total strategy package by the inclusion of another approach -- something closer to Strategy 4 and perhaps akin to what Anderson is advocating. And because of their attendant advantages, the government should probably be alert to situations in which the pursuit of Strategies 2 and 3 might make sense, as well.

So perhaps, in our quest for improved information security, our specific destination is now in view and our route is less obscure. But it is one thing to decide where one wants to go, and quite another to overcome the ever-present obstacles and actually get there. Even when a course is perceived as inevitable, rough terrain and all forms of hidden traps and required detours can render that inevitable destination elusive for a very long time. The next chapter looks at the forbidding terrain and some of the traps and detours that may lie in our path.

Chapter 11

If We Know Where We Want To Go, Why Don't We Get There?

The previous chapter discussed various strategies that the government might follow in pursuit of information security. These strategies were presented as if the government had the power and freedom to choose. This is far from clear. The success of any selected government strategy will be largely determined by the extent to which industry cooperates with it. But industry is unlikely to move very fast, regardless of government pressures, unless the business community, which represents the dominant share of the industry's market, evidences a strong demand as well. Walker made this point at a May 1982 conference:

. . . it is absolutely crucial that the manufacturers get pressure not just from the Defense Department for computer security, but also from the banks and financial institutions If we [the DoD] start asking for things that are useful only to us . . . , the manufacturers are going to resist, claiming we are too small a part of the market.

And the business community, unless forced by law or government regulations, seems to prefer to proceed cautiously, procuring only those mechanisms that are patently cost effective. The business community cannot be expected to be in the forefront of demand for security products unless those products are perceived to increase profitability. With respect to these products, business appears to be far more comfortable riding the government's coattails. In other words, the contributions of all of the three sectors are so interconnected that it is very difficult to judge which sector is in the dominant role.

With respect to the separation issue, even if the government, industry, and business should jointly decide that COMSEC and COMPUSEC should merge -- that the two should be pursued as one -- a merger is probably not all that simple. Historical and even cultural differences are likely to render such a consolidation most difficult to achieve. This difficulty could even increase as the separation continues.

Thus, government and business may not be unrestrained in their pursuit of a selected strategy. This chapter examines some of the constraints that are likely to bind the strategy choices of both government and business.

In two of the alternative strategies discussed in the previous chapter, the government would decide what it wanted and then pay industry to produce it. A major factor inhibiting the success of such a strategy -- even setting aside the government's problem in deciding -- is that many companies would have no interest in such an arrangement. Steven B. Lipner of the Digital Equipment Corporation (DEC) spoke for such companies when he said, "I give you the hardest challenge I can think of: write a federally-funded R&D contract with us." When asked why his company would not accept government R&D money, Lipner replied:

I shouldn't say that so absolutely. Historically, we have funded all of our product research and development internally That [accepting the government's money] is something we've just never done, and⁶³ . . I don't particularly perceive a change in that.

He was quick to add, however, that this was only his own perception and that others in his company are known to hold a different view.

SRI's Peter Neumann offers one reason why industry is not eager to accept the government's money:

There's no real gain in it. They [industry] perceive over and over again that the amount of profit that they're going to make is strictly what they can do out of that system development effort plus the few they can sell to the government. But, they're never going to have that as part of their main line -- because nobody wants it (or at least so they profess).⁶⁴

According to Neumann, a cost or risk sharing approach is not likely to work either. Neumann compares the situation that exists in computer security with that of the VHSIC program:

. . . there [the VHSIC program], the computer vendor has the opportunity to do something that's going to benefit every single piece of his product line, whereas in the computer security business, the vendors are saying, "Hey, we don't need that. None of our customers want it. Why should we have to waste our time producing something for a government client who's only five percent of our business?"

The problem appears to be one of perception. Neumann himself says, "I don't believe it's true that nobody wants it." But he indicates that this seems to be what the producing industry believes. Citing the example of IBM, Neumann says:

Apart from the System 38 guys, who are apparently out of the mainstream, nobody is really worried about it [COMPUSEC] because they [IBM] continually believe that the banks, the real commercial buyers, do not need it. . . . IBM says, "We don't care, because we can't sell it commercially."⁶⁵

Even among companies that would be willing at least to consider such an arrangement, there are those who foresee some serious costs involved -- particularly if the government insists on cleared facilities as a way of coping with the subversion threat. Sperry-Univac's Theodore M. P. Lee, for example, stated in an interview:

. . . the idea of having to operate an entire main-frame computer assembly-line and operating system programming staff in a fully cleared environment would be so expensive as to be ridiculous. It would be feasible only if the government were convinced that A1-level systems were so essential to national security (including economic security) as to justify it, and that the threat of subversion . . . were real enough that nothing less would do.

He then added, "I'm skeptical about both. . . . I'm just guessing the government couldn't afford to spend the money we would ask them to, for us to do that."⁶⁶ In actual fact, as far as Sperry-Univac is concerned, the problem for the government is even more fundamental. When Lee put the question to his senior management, the answer came back that the company might accept government money to do an A1 system but would be unwilling to do it "under conditions in which most people had to be cleared."⁶⁷ In other words, one company, at least, might cooperate with Strategy 3, but not with Strategy 4. Clearly, the government does not have an unrestricted choice of strategies.

Even with Strategy 3, the government may not be able to come up with enough money to make it worthwhile from industry's point of view.

Lee explains:

One point concerning the feasibility of the government's deciding to assume the development risk (whether in a cleared environment or not) is that the cost to industry of doing it that way is not just the direct cost of what it takes to get the job done, including the cleared facilities, but also the lost opportunity cost of our deciding to use scarce people ⁶⁸resources . . . on that task, rather than on something else.

The two other strategies discussed in Chapter 10 involved the government trying to goad industry into underwriting the development itself. These strategies do not look all that promising, either, at least in the near future. The Director of the DoD Computer Security Evaluation Center (CSEC) recognized the inherent difficulty when he said, "To divert the momentum of a highly competitive industry whose market is doubling every five years to a 'trusted' product line is a formidable task."⁶⁹

The first hurdle that the government seems to face upon telling industry that it wants secure products, is convincing industry to

believe it. When Lee was asked if he believed what he was hearing from the government, Lee replied, "I personally believe it." He was quick to add, however, "I don't know, necessarily, that I can convince the decision makers . . . in the company that I believe it." Lee attributes much of the lack of belief to the fact that DoD procurements for information systems contain little in the way of security requirements.⁷⁰ He noted that his company had, in the previous six months, acquired \$2 billion worth of new government business. Referring to two large recent contracts, one with the Air Force and the other with the Navy, Lee stated, "Neither one of them had any significant security requirements in them." While admitting that he did not know whether they should have had or not, he points out, "You can see that the guy who's counting the bottom line says, 'If I can make a lot of business that way, I don't have to worry about these problems.'" Still, Lee admitted that the perception was gradually changing. "I think that enough people are beginning to believe that it's something more than just smoke and noise," he said.⁷¹

Even if industry were to come to believe what the government was telling it, there would still be a reluctance to jump too far in front of today's commercial market. If industry is unwilling to develop an A1 system with the government's help, then it surely is not likely to do so entirely on its own. Industry is just too afraid of ending up with a technological curiosity -- a state-of-the-art white elephant -- that a few esoteric government customers might buy but which could not be sold to anyone else.

So industry is proceeding, ever so cautiously, to include a little more security in its products. Largely unmoved by the government's

voice, but egged on by COMPUSEC advocates within their own companies, industry inches its way, incrementally, up the security levels of the CSEC criteria, always moving at its own comfortable pace and careful not to tread dangerously ahead of business' stated needs.

One DEC engineer told a government-industry audience, "Digital is interested in evolvable security. We want to evolve existing systems to become more secure." He went on to explain some of the rationale behind the company's strategy choice:

In terms of evolvable security, it is very important to us that security features fit in with our existing products. DEC has been in business quite a while. We have been selling PDP-11's for well over ten years, and we have been selling VAX's for several years. Not only do we have a lot of investment in that software and a public commitment to its stability, but our customers have an enormous investment in their own software that uses our operating systems. We must be very careful not to invalidate customers' software with future security enhanced products; doing so would severely discourage the market for such products.⁷²

This evolutionary pace is likely to continue unless and until business articulates a strong requirement for enhanced security mechanisms.

But while industry waits and listens for the voice of business, business remains strangely mute. As Lee puts it, "They [the business community] aren't saying much. . . . I don't think they really know what their problems are and that they need to solve them."

"Hypothetically and in practicality, I know . . . you can go down to the computer system at almost any company and open it up," says Lee. But he asks, "Is that really a serious risk compared with all the other risks?"⁷³

IBM also reports that the demand from the commercial sector has been weak. In fact, according to DeMaio, IBM consistently includes

more security in its products than its customers are demanding -- often in response to IBM's own internal needs. DeMaio states:

. . . the entire security marketplace has been pretty much driven . . . from a sense of what a responsible manufacturer has to do in the marketplace as opposed to what the market is clamoring for in a business . . . sense Most of us [computer manufacturers] have to look very hard at the rules on business justification, in order to get security out the door. . . .⁷⁴

According to consultant Robert P. Abbott, apart from an obscure clause in the Foreign Corrupt Practices Act,⁷⁵ "there isn't anything that requires the private sector to do anything about computer security. . . ." Says Abbott:

The motivation comes of protecting those dollars -- of protecting those assets and avoiding law suits. That's the only motivation. If there are risks associated with it, the risks have to be weighed against the cost of absolute protection, and quite frankly, they're going to come down on taking risks, most of the time.⁷⁶

Abbott relates his experience when he first set himself up in business, several years ago. "I was told by bankers that, obviously, you could not steal, except from a depositor's account, and a depositor's account is insured by the FDIC." According to Abbott, this shows that private industry is prepared to accept risks and "is not necessarily motivated to spend money -- particularly when it doesn't produce revenue."⁷⁷

The way business sees it, the mechanisms that industry has to offer are not likely to be of great help. The Bank of California's Leslie S. Chalmers states:

From the point of view of the banks, our biggest security problem is our ability to control our employees, and that really does not get answered by secure operating systems. It's not the kind of problem that you can necessarily correct with encryption.

In Chalmers' view, what banks need more than technical mechanisms are procedural and audit controls.⁷⁸ IBM's DeMaio agrees. He points out that the businessperson is often more concerned with auditability than with what DeMaio calls the "preventative aspects" of security.⁷⁹

Nevertheless, some requirements for security mechanisms have been stated. Says Lee: "I know we have some contractual commitments that mean, as I understand them, [we] are really going to have to do a B1 in something like two, three, or four years."⁸⁰

The development of even reasonably robust data security products is not a trivial undertaking. It requires the commitment of a company's scarce resources, both people and money. There is an understandable reluctance to commit a scarce and expensive resource to a product whose marketability is so poorly known. Not surprisingly, industry is limiting its investment. Speaking for DEC, Lipner says:

We are exploring what one might do to provide a security kernel that would be at a level of investment consistent with what we think that market is. . . . Since we are resource limited internally. . . . I can't envision a big effort for a potentially low-volume product.

Industry perceives an interest in more robust products but it fears that the extent of that interest will be very much influenced by price. The DEC strategy, therefore, is to build as much additional security into its product as possible without appreciably raising the price of the operating system above what its customers are used to paying. Says Lipner:

If you have to charge 100 thousand or 500 thousand dollars a copy to recover your investment, the risk would be too high. . . . There is too much of a chance that a competitor would beat you on price-performance ratio. So we would rather build something that would sell within a reasonable price range for an operating system or a system utility.

Rather than raise the price, Lipner seems to prefer accepting some modest cut in performance:

The place where we might ask people to pay a premium . . . might be in performance. There might be some performance penalty to running a kernel, either in the sense that you would have to run somewhat slower or buy more memory or discs . . . or both. But, we can't degrade a [VAX 11-] 780 into a [VAX 11-] 730 and that is, in fact, . . . the highest risk associated with a security kernel development.⁸²

The problem for industry in assessing the market for security-enhanced products would be bad enough if some homogeneity in application systems existed. The fact, however, is that even within a single business, there is a wide diversity of products or systems. Speaking for what he called the "wholesale" banking business, Citibank's M. Blake Greenlee stated, "Typically, we have a different processor for each type of banking product for each type of banking customer."⁸³

Furthermore, business needs tend to change rapidly as they strive to keep pace with the changing requirements of their own customers.

Says Greenlee:

Our customer requirements change rapidly. We find that any system that cannot be produced and put on line for the customer in six months' time is not worth developing. Put another way, if the project manager walks in with a milestone chart and the date for live operation is greater than six months out, the project is cancelled because the environment will have changed so much in that time that it won't fit customers' needs.⁸⁴

No one is going to turn out a secure information system in six months.

Business also places high values on ease of operation and on support. Addressing her remarks to the computer industry, Chalmers states:

If you do come in our door and you want to try to sell us a product . . . you'd better jolly well have your act together in terms of being able to demonstrate that your

product is reliable, that it's easy to install. I mean really easy -- off the shelf -- no modification. We want to be able to drop it in without any work at all . . . and we want support. If that thing breaks, you've got to be able to fix it in a timely manner.

There are, in fact, vendors with whom we would prefer not to do business, because they simply do not support their product. They assume they are still selling to college, university type populations; and, if their computer breaks, that you will take off the side panel, roll up your sleeves and wire it. Whereas, in fact, when we have something that breaks, . . . we roll up our sleeves and pick up the telephone. And that's the way we intend to keep it!⁸⁵

The implication of all of this is that it now appears that the government will have to endure a painfully slow evolutionary process within industry, which might well never converge with the government's ever increasing need -- or even its present need, for that matter. To the question about whether he saw a market for A1 and beyond products, IBM's DeMaio answered, "I don't know," and then added, "We're still in the throes of trying to determine whether A1 is technically feasible."⁸⁶ And when asked if he foresaw his company ever producing an A1 system on its own, Lee replied, "I don't know. . . . I know there are enough people who are concerned about it as a possibility." But, he added, "I don't know if it's even a practical thing to consider for the large-scale systems we do." Nevertheless, he expressed his own opinion that if his company were to decide to do so, it could produce an A1 level product in "five to ten years." Although he admitted that no such decision had yet been made, he thought it would come soon or not at all. "If we don't have it [an A1 level product] 10 years from now," he says, ". . . it probably means that it's not going to happen."⁸⁷

And Lee was speaking only of an A1 product. For some applications, even today, the need is for better than that. The fact

is that many present environments require exactly those robust security mechanisms that are deemed beyond the state of the art -- mechanisms beyond the A1 level. Perhaps with the "right" strategy the government might advance the arrival date somewhat, but even this is far from certain. What is fairly clear is that so long as the Computer Security Initiative, or Strategy 1, effectively constitutes the sole government strategy in the field of computer security, there will be no A2 or better systems.

One of the major stumbling blocks in the building of an A2-level product appears to be code-level proofs. The criteria for systems beyond A1 ultimately require that formal verification be carried down to the code level.⁸⁸ However, except for a few very small programs, this has not yet been successfully done. This problem is largely independent of the government procurement strategy. But there is another consideration. A rating beyond A1 will also require that the Trusted Computing Base "be designed in a trusted facility with only trusted (cleared) personnel."⁸⁹ It is this requirement that dictates a strategy other than Strategy 1. In particular, it demands the cleared environment of either Strategy 2 or 4, both of which seem to have been rejected by industry. And even the cleared environment may not be enough.

The purpose of the "trusted facility" is to cope with the threat of subversion. But subversion is likely to prove exceedingly difficult to contend with -- assuming there is someone out there who is attempting it. As Neumann points out, "It's a very humbling thing when you think about all of the very easy ways one can subvert a system."⁹⁰ As was indicated in Chapter 8, either hardware or software can be

subverted. However, from the subverter's point of view, subverting the hardware probably constitutes the better strategy. Hardware is more difficult to verify, is more likely to be overlooked, and is usually more permanent. One technical article states:

Correct functioning of the access control software depends on correct operation of the hardware. . . . No reasonable methods for verifying that the computer system hardware is functioning correctly are known. It appears to be a relatively straightforward matter to modify the hardware so as to invalidate the access control mechanisms of a computer system.⁹¹

And Neumann adds:

. . . people tend to trust hardware more than software, and very few people seem to realize that the algorithms can be wrong in hardware just as they can be wrong in software.

The hardware changes less often, so you do have a chance of getting at it in a relatively permanent way, whereas with the software, you may find that a penetration . . . works one day and . . . doesn't work the next. Nevertheless, hardware changes can easily be installed during routine maintenance, for example, by replacing one board with an almost identical one containing a Trojan horse with a memory that squirrels away information that can be stored until the next maintenance visit.⁹²

In an interview, Lipner related his 1972 experience as a member of the MULTICS penetration team. One of the penetration routes that the team discovered took advantage of a flaw in the hardware. The team designed and ran what it called a "subverter program," which would activate itself at regular intervals, searching for random hardware failures. Although it found none, it did uncover a subtle and previously unknown hardware flaw that permitted a penetration.⁹³ There was no reason to have suspected that the flaw had been deliberately placed there, but the incident points up the general vulnerability to hardware subversion.

This vulnerability has probably grown worse in recent years.

Lipner states:

The problem [hardware subversion] worries the hell out of me, because our processors have not gotten simpler in the last ten years. Nobody's have gotten simpler in the last ten years.⁹⁴

Lee agrees:

It's probably reasonable to say that there weren't any Trojan Horses [illicit programs to exploit the system] planted in software that was [written] about 15 years ago. It wasn't necessary and it wasn't a meaningful thing to think about doing. So certainly, there's a larger chance that there's a Trojan Horse in our current operating system than there was in the one 15 years [ago]. [However,] . . . there's enough noise in the whole process, you could argue that any Trojan Horse⁹⁵ that was put in there somewhere . . . long ago got killed.

Lipner believes that the government's new computer security evaluation criteria are not properly balanced -- that they demand more of software than they do of hardware. Says Lipner:

I believe they should have a set of requirements for the hardware as well as the software. The current stress on software and neglect of hardware issues seems way out of balance and perhaps even unrealistic.

"But," he adds, "if you say, 'Build the hardware in some secure environment,' you're not going to get any hardware, I don't think." As Lipner explains, "If I . . . have to get even a modest level of security clearance for all of my people, that's probably a stopper." According to Lipner, the problem is environmental. Lipner believes that classification and access restrictions would be perceived by his employees -- even by those who were granted the clearance -- as stifling. Moreover, Lipner fears that not all would obtain the clearance, some by their own choice. As Lipner himself summarizes, "For all those reasons, it's perceived as an unattractive kind of environment."⁹⁶

Nevertheless, Lipner offers a way that the government might obtain DEC hardware that was built in a secure environment, without requiring

DEC to build it. The mechanism he suggests is licensing. According to Lipner, DEC already has licensing agreements with at least two companies. The Norden Co. builds militarized versions of three models of the PDP-11 and both Norden and Raytheon build militarized versions of the VAX. Although these militarized equipments are not classified, Lipner points out that both companies are qualified government contractors, both have facility clearance, and both have "lines where they can produce classified hardware." He feels confident that either company would willingly accept the government's money to produce DEC computers in a restricted environment. Lipner concedes, "At some level [of certification, e.g. A2], classified production of hardware might become necessary . . . and that [licensing] may be a mechanism that may be workable."⁹⁷ A difficulty with this idea is that simply to reproduce the same design in a secure environment may not solve the problem. The design may already contain the subverted flaw.

The bottom line seems to be that if the government continues to pursue Strategy 1 for COMPUSEC -- the strategy of the Computer Security Initiative -- it may never get a second A1 product, that is, other than the Honeywell SCOMP. And even if it does get such a product, it will not get the product very soon. As Lee puts it, "It [the Computer Security Initiative] is not going to get you an A1 very fast."⁹⁸ Any product beyond A1 appears to be out of the question.

Strategy 2 (classified environment with industry bearing the risk) does not look at all promising, either. Industry shows little interest in a classified environment and seems willing to bear the risk only for a product that it can sell openly.

Strategy 3 (government sponsorship and unclassified environment) may well result in a product somewhat faster than Strategy 1, but the product will not meet the requirements of an A2 system.

Finally, Strategy 4 (government sponsorship and classified environment) might work if the government is willing to accept a product from a company other than the one that designed it. However, the pursuit of this strategy will require of the government significant changes in philosophy, in strategy, and in commitment. It is likely to be very expensive. A product designed to cope with subversion could cost 50 to 100 times as much as the government is accustomed to paying for non-secure products of similar functionality. There is little evidence of this level of commitment. Earlier, this report mentioned the government's balking at a 10% increase.⁹⁹ Admittedly, this 10% was to be applied to all DoD computers, whereas only a small number would require better than an A1 rating. Nevertheless, it suggests that the government's level of commitment is very much affected by price.

And then, there is the matter of separation. Eliminating the current separation between the worlds of computer security and communications security will not be easy, either. As Harold J. Podell of the GAO points out:

There is reason to believe that the historical separation of computer security and communications security will be very difficult to bridge for a whole variety of reasons. One is the knowledge base of computers is historically different than the knowledge base of communications, even though they're merging. They're coming from different parts of technology.¹⁰⁰

Some of the separation is simply a reflection of a long-standing rift between the communications and the computer communities. The

separation runs deep and the atmosphere between the two communities is not serene. A great deal of mutual distrust and suspicion seems to have permeated their respective security communities as well. Within the entire communications field, computer people have always been the "new kids on the block." Generally, they have more education than do communicators whereas the communicators tend to have more experience. When two social groups -- one heavy on experience but light on education, and the other light on experience but with more education -- are intermingled in a working environment, working relationships often become strained. Most organizations that have bowed to the logical (and inevitable) by combining their communications and computing functions have found the desired synergy to be quite elusive.

Communicators and COMSEC specialists have had decades to work out a reasonably amicable coexistence. Communicators and computer specialists have not had as long, and their relationship is still strained in many organizations. COMSEC and COMPUSEC people often come from different backgrounds and, as has already been discussed, have quite different goals and strategies in mind. But the strain seems to be greatest between communicators and the practitioners of computer security. COMPUSEC is an even newer field than computing itself and its specialists are typically highly educated in computer science, only further aggravating the rift.

One of the effects of this rift is that large existing communications systems are not benefiting from what COMPUSEC might offer them. In particular, according to Anderson, communicators are presently resisting the imposition of computer security standards and are trying hard to wriggle out from under them. (Ironically, members

of the COMSEC community have feared that any standards set by computer security people would be too loose.¹⁰¹) "They don't want the same standards to apply," declares Anderson. "Their resistance is based on the perception that they're going to lose turf in this battle." According to Anderson, "It's not . . . that anyone really objects to the criteria. They object to its being imposed . . . within the next 25 years or so." He explains:

They [the communicators] have been at the game a long time and they think they have all wisdom. They really don't see that computer security types can really add to what they already know. They think they know it all.¹⁰²

The battle over turf seems to extend to the two security communities as well. To illustrate the nature of the battle over turf in which the COMSEC and COMPUSEC communities are engaged, Anderson offers the example of some computer security people who wished to encrypt computer files by using the DES algorithm. A dispute arose over which group would issue and control the cryptographic keys. The COMSEC people maintained that the generation and control of cryptographic keys was a COMSEC function, thus they should have jurisdiction. The computer security group claimed that it should be in charge since the protection of computer files was involved.

When asked if he foresaw a solution to the rift problem, Anderson was pessimistic. "It's an issue that's so politically charged [that] it will [require] a directed solution that will satisfy no one," he said.¹⁰³ When Anderson speaks here of this problem being "politically charged," he is talking about the low politics of bureaucratic infighting. This seems to be an example where the intrusion of low politics acts to block the intent of higher authority.

Separation may be a larger problem for the government than it is for industry. Although some admit to a separation within their companies, others such as Lipner of DEC do not. According to Lipner, a separation of the relevant technical work does not exist within DEC. He says that when he was hired into the research group, he was to manage research projects in both operating systems security and in network security. While admitting that the network security work has since been "spun off" to the network department, Lipner states that his group continues "to track their progress, [to] work with them, [and to] review their documents." Lipner concludes:

We're not separated. . . . At the level of an individual product -- a board, a module or a box -- you have to have enough separation to get something built and shipped, but . . . at the level of architecture, ¹⁰⁴ interoperability or standards, we don't separate.

However, Lipner injected a most important qualifier, which returns to the matter of strategies. He foresaw an immediate difficulty if integration forced upon the COMPUSEC industry the development strategy of COMSEC.

If the government integrated them in such a way that, to do serious computer security, we had to do classified development, for example, that would have a major impact on us.

As Lipner explains, "If I build a security kernel, and there's a market for it outside the government, I'd like to be able to sell it."¹⁰⁵ So, it would seem that the strategy issue and the separation issue are linked. The attainment of adequate information security within the government -- if not within business as well -- may depend upon finding a satisfactory means of coping with both issues.

Meanwhile, the problem of information security does not remain stagnant and waiting to be solved. All dimensions of the problem race

ahead, become more complex, more interdependent, and more urgent. For example, within the national security sector of government Project Air Force 2000 has called for increased initiatives "to integrate computer and communications systems throughout the Air Force."¹⁰⁶ And in the commercial world a whole new industry is developing around efforts to interconnect computers. Companies have formed with no other purpose than to interconnect computers in a common network.¹⁰⁷

Such developments surely have security implications. Gordon Welchman writes:

In the 1970s, and particularly in the second half of the decade, there was a revolution in the technology of communication, and in the recognition of what communication is all about. But what we have seen so far is only the tip of the iceberg. We must expect major developments in the 1980s, and they are sure to introduce new security problems.¹⁰⁸

Actually, they already have. It is just that only now are we beginning to understand what the problems are.

Information security represents one of society's most difficult technical challenges. A satisfactory technical solution to the subversion threat, particularly to hardware, probably lies beyond the state of the art, at least through the 1980s. The interdependence problems of automatic key distribution and of label guarding remain formidable. Communications channels are vulnerable unless these problems are solved; yet the solution to both seems to require a trusted computing base -- which, again, for certain applications, means better than an A1 system. And no one has yet found a way to avoid the particular type of confinement problem caused by the need for some address information to bypass the encryption process in a PLI-like device.¹⁰⁹

Yet information security is much more than a technical problem. The legal and social problems attendant to information security are as elusive as the technical ones. For example, given that the law requires the federal government to protect the information it retains about its citizens, what constitutes appropriate protection in a legal sense? We already know that we cannot soon achieve adequate protection for all information in a technical sense, i.e., equal to the potential threat. But might not the legal standard be somewhat lower? How is this legal standard to be determined? By whom?

Among the legal standards now being applied is that of "due care." The idea behind "due care" is that the directors of a company can be held personally liable for the loss of assets if the loss could have been averted by the exercise of "due care" of the assets. According to one trade publication, encryption has already "almost become a standard of 'due care' for banks." The publication also notes that the application of the "due care" standard has not been restricted to financial institutions.¹¹⁰

The social issues, too, seem major. Some insight into the scope of the problem is revealed by the following excerpt of a magazine article by George I. Davida, a professor at the University of Wisconsin:

. . . some credit card systems are now on line, and more are sure to follow. Even today it is possible to track a citizen of this country month-by-month and week-by-week through bank records and credit card charges. In fact, at least one fugitive from justice has already been apprehended in this way -- he had eluded pursuit until he made the mistake of using his Master Card. When all the credit card systems go on line, it will be possible to track people hour-by-hour; every time one's target made a purchase, one would know where he was and what he was up to. . . .

Indeed, all this computer data is so vulnerable, so easy for a clever outsider to tap, monitor, and even alter

or erase, that we are rapidly moving toward a world in which George Orwell's nightmare, a totalitarian state with almost supernatural surveillance systems, becomes a technological possibility.

Although his words contain a somber warning regarding what might ultimately become possible, Davida seems to be guilty of exaggeration for the sake of emphasis. It is true that virtually all computer data are alarmingly vulnerable. But even the penetration of vulnerable data is not without some cost or some degree of risk, both of which rapidly increase as the scale of the penetration is enlarged. It is one thing for a single, private individual to gain one-time, deliberate access to a computerized data base and to achieve whatever mischief he or she might have in mind. It is quite another thing for an individual -- even a well-financed one -- to gain wholesale and repeated access to that data base.

Even governments are limited in what they can accomplish. In the credit card example, law enforcement authorities had the luxury of being able to focus on just one individual. And, as Davida points out, they succeeded. But this incident should not lead to the conclusion that a government -- either ours or another -- would be able to keep track of an entire population. Perhaps it could, but Davida's example does not prove it.

Nevertheless, this example does illustrate the potential danger to individual liberty and freedom as the capability mounts to accumulate large amounts of accurate information.¹¹² Yet this danger multiplies when the information accumulated is inaccurate -- when it is distorted either by lack of care, by technical error, by random mischief, or by deliberate and directed alteration.

Recognizing the technical challenge involved in solving the total information security problem, suppose we were to give up? Suppose we were to acknowledge that the solution is simply too difficult -- too costly? What, then, would be the social implications? Could we be heading for an era when all must presume that everything we say and all that is stored about us is likely to become known? According to one writer:

The individual needs personal autonomy. He needs the emotional release of "off stage" moments when he can be "himself," free of the various roles he plays in his daily life. He needs limited and protected communications.

If Davida is even close to being right, he may not get them. At least, he may not know whether he is getting them or not. He, and the rest of us, would then face an unknown risk. In fact, we do now.

But how is this different from other aspects of everyday living? Life is hardly risk-free. Modern society lives with risk every day, most of which defies quantification. How would one quantify the risk of unintentional nuclear war -- or intentional nuclear war, for that matter? What is the chance that the next time we drive our car home from the movies some drunk driver will suddenly loom in our path? How can we measure the likelihood that the air we breathe in today will become the spawning ground for a mortal cancerous growth? The facing of unknown risks is and has always been part of life. There are always heroic -- and usually extremely costly -- actions that we could take to reduce these unknown risks, but most of us do not take them. We simply learn to subjugate our concern about these risks to a level that permits daily functioning. We will most likely learn to do the same with the threats to our privacy that imperfect information security protection portends. Nevertheless, as with all of the other forms of

societal risk, we should constantly strive to know the extent of the risk and to take reasonable measures to limit them.

Custodians of data would seem to face quite a different problem. Since the privacy they protect is not their own, the protection vs. cost tradeoff should perhaps not be left to them alone. Custodians probably should not be free to trade off the protection of someone else's data against the cost to themselves. The social issues that attend information security are not as easily dismissed for custodians as they might be for individuals.

Finally, there is a moral or ethical dimension to the information security problem. In fact, of all the aspects of information security, this may be the most disturbing. With the advent of the information age has come a new literacy characterized by the attainment of a set of new information skills.¹¹⁴ Educational institutions, recognizing the importance of this new literacy, have responded with new courses. And employers have been willing to reward the attainment of this new literacy with higher salaries.

But the new literacy seems to be accompanied by a new morality as well, a morality that sees illicit accessing of someone else's computer files as morally neutral. The new morality has spawned a popular new hobby -- computer hacking. Many hackers are intrigued by the challenge of gaining illicit access to computers. They have created their own underground network and even have their own newsletter "TAP," which, among other things, provides telephone numbers and entry details for institutional computers.¹¹⁵

Most hackers do not intend to inflict harm. As soon as they are satisfied that they are able to accomplish whatever they set out to do,

they usually quit. After all, at that point the challenge is gone. Their activity is somewhat analogous to that of a person who enjoys breaking into buildings but never takes anything. The ethical question is whether there is anything wrong with simply gaining access to someone else's file so long as no one is harmed, i.e., no data is destroyed and no action is taken based upon information so obtained.

In the analogous case, U.S. law recognizes the act of "breaking and entering" as separate from the act of burglary. Yet it defines both as crimes. It seems to recognize the sanctity of one's home or business even if nothing is taken. There appears to be no crime corresponding to breaking and entering statutorily defined for information systems. There is also not the risk of physical harm that exists in the case of illicitly entering a building. Perhaps this explains why many who engage in hacking see nothing wrong in it. As a 1983 Wall Street Journal article puts it, "Die hard hackers say there isn't any harm in any of this, provided data never gets destroyed and no one gets hurt."¹¹⁶ Some, like MIT's Richard Stallman, even seem to condone malicious hacking. The Journal article records:

The malicious hackers, says MIT's Mr. Stallman, may simply be rebelling against antisocial "fascist" computers that seek to keep users out. "I call him a person who has been alienated by the hostile atmosphere he perceives in most computer systems," he says. "He reacts to it with anger, which is perfectly justifiable, in my opinion." . . . "It's as if you're playing a game," says . . . Stallman. "When they [security people] start playing that game, they shouldn't be surprised when other people play the other side."¹¹⁷

Angeline Pantages, writing in Dun's Review, summarizes the problem of ethics thus:

Ethics is probably one of the most controversial subjects in the computer field today. A corporation cannot assume uniform standards of ethics among its computer staff.

This does not mean data-processing professionals are crooks, but, short of theft of money and goods, they don't always agree what constitutes a high ethical standard.

The author attributes some of this ethical ambivalence to the industry's early days, "when computer programs were frequently exchanged because of the lack of software." Her claim is that, until recently, software was even exchanged among competing service companies.¹¹⁸

Pantages also assigns some of the blame to university computer science departments, which, she says, "have encouraged 'computer busting' -- finding ways to gain unauthorized access to the system," and have even made such a practice an assignment. Referring to a case at the University of Alberta in Canada in which two students were prosecuted for gaining repeated unauthorized access to commercial accounts serviced by university computers, after allegedly having been encouraged to do so by some of their professors, Pantages notes:

This case was the focus of a discussion at a recent National Computer Conference in New York. At the session, the industry's professionals demonstrated a wide range of disagreement on whether to teach students to break the system. One professor defended the creative benefits and even denied university responsibility for those who took the assignment too far. "We are not here to teach ethics; they should have learned them before they arrived on campus," he argued.¹¹⁹

The professor is probably right in saying that ethics should have been learned before college. In fact, they almost surely are. However, what is being learned may well be the "new morality," which seems to be acquired at an early age. Peter S. Browne, Vice President of Burns International Security Services, had this to say:

I have had firsthand experience with this, because my 14-year-old son is a budding technologist with a home computer. I shudder at the practices that he and his peers at school accept as common, normal, ethical -- like the pirating of

programs. No one has told him it is wrong, except his parents. All of his friends do it. I have great concern about schools that give the impression it is acceptable to hack at systems.

Computers are games to our children and it is just a matter of changing from a Mattel toy to an Atari toy.¹²⁰

Computer security consultant Donn B. Parker articulates some of the obvious ethical questions that arise. Referring to the "system hackers . . . who have learned to compromise computer systems from the telephone and from terminals in high school," he asks:

What are these people going to do as they become our trusted technologists? What kind of values are they going to carry with them when they have learned that it is acceptable to attack systems, to technologically trespass, to engage in computer program piracy?¹²¹

When Chalmers demanded "support" from computer vendors, she was requesting both maintenance and regular updating of software.¹²² Having already admitted that banks have learned painfully that they cannot completely trust their own employees,¹²³ she seems willing to trust outsiders to build, maintain, and update her bank's computers. To an outsider this may sound bizarre indeed. But her demand is not at all unusual. It merely reflects the way that business is typically conducted within the computer world. The problem is one of galloping obsolescence. Not much in today's society becomes outdated as fast as a computer. To hedge against a prospective customer continually waiting for the latest model with the newest feature, computer manufacturers have had to commit to a high degree of support. Software, particularly, is constantly upgraded and improved. Bugs or flaws are found and corrected; new capabilities are added. This process of support begins the day a new product is announced. When it stops, customers are forced either to replace the product or to take

over the support themselves, a function that few are prepared to assume.

But an environment that permits such flexibility and change is not an environment conducive to security. Security wants stability -- even rigidity. It generally prefers any known risk to an unknown one. For example, when designs were being considered for a binational intelligence system, the DoD accreditation official argued for a known, older system with fewer security features over a new design with more built-in security-enforcing mechanisms. "You don't need to take this risk," he is quoted as saying.¹²⁴

Clearly, the standard way of conducting business in the computer world was not designed with security in mind. Depending upon unknown persons from outside organizations is surely taking a large unknown risk. What reason is there to expect that unknown outsiders are more trustworthy than known bank employees whom banks have learned cannot always be trusted?

The problem is that many of today's system hackers are likely to be tomorrow's designers of information security products. If they are guided by the ethical values of the new morality, can we afford to trust the products they produce? Yet if we cannot trust their products, whence will the needed products come?

And even if the secure products do come, the state of information security might not be appreciably advanced. There is still the "human problem" to contend with. As Neumann states, "I think there are many human problems that can completely undermine even the best secure computer system and network."¹²⁵

Speaking about the achievement of information security within the business sector, SRI's Donn R. Parker had this to say:

Even if we train end users and give them the proper controls, how are we going to motivate them to use them? You know, security is getting a boost from commercial software packages. Internal controls are becoming major features in the sale of these packages, and the question will become, "Will the user turn the controls on, or will he turn them off for the convenience of getting a job done more cheaply?"

I contend that the controls won't be used until these people are sufficiently motivated. I think motivation has to do with how people are measured in their jobs. If you measure an employee by how many widgets he produces, he is going to produce as many as he can. If controls get in the way, he'll beat you every time. Security won't work unless the employee is judged not only on his production, but also on how safely and securely he does it. ¹²⁶

And referring to government agencies, Neumann states:

Even if we had an ultimately secure computer system maintaining multilevel separation, e.g., in inferential databases as well as computer systems in general, many people would find it difficult to use such a system simply because they do not understand their own security requirements (which are, then difficult to translate into computer requirements). ¹²⁷

Neumann goes on to say that he is convinced that there does not exist a technical solution to the human problem. "I don't think you can solve the problem," he says. "I think you can ameliorate it." Neumann adds, "There are just too many ways of screwing up, accidentally or intentionally." Neumann concludes with this pessimistic observation:

. . . in some sense, you should never trust a computer to maintain security. No matter how clever it is, it's the people who will always be able to misuse it. And, if you have something that's very sensitive, you probably shouldn't ever put it on a computer. ¹²⁸

Yet everyone -- including the national security sector of the government -- does, and probably always will.

While it is true that a system does not have to be automated to suffer from these human problems, the problems tend to be magnified when information is massed within large, monolithic information systems. As a GAO report has noted:

The potential for misuse of information by individuals in positions of trust is not unique to automated processing systems -- the problem exists in manual systems as well. Nevertheless, the concentration of information in automated systems increases the magnitude of the risks . . . and additional controls are necessary.

Information security truly remains an elusive problem.

So where are we heading? In looking ahead at what might lie in store for information security products, three possible courses or scenarios appear.

The first possible course could be characterized as "no real change." Under this scenario, COMSEC and COMPUSEC continue to be seen as complementary but remain essentially separate. Only systems designed and built for very special applications under strict government control are considered truly integrated in an information security sense. There is a temporary flirtation with the few commercial products that are now being developed, but they prove unpopular. In general, those government and non-government organizations concerned about information security choose a tightening of administrative and physical controls over technical measures. This outcome is likely if, for whatever reason, the marketplace becomes disenchanted with or comes to distrust the current new products and decides to return to the controls they better understand.

The second possible course of action could be described as "continued slow progress." Under this scenario, industry continues to make modest but helpful improvements and these successively more robust

products begin to find an increasing market -- first, within the national security sector of the government; then, in certain of the more demanding businesses like banking; and finally, within the broader range of more mundane government and non-government applications. The market fails to take off but it does become slowly and steadily stronger. A few companies opt out but a sufficient number stay in to assure the government and business of a sufficient range of products with varying degrees of security robustness. The problem of subversion is effectively deferred. There continue to be no information security products that even claim to offer much in the way of protection against this class of threat. From today's vantage point, this course appears the most likely.

The third possible course could be depicted as "rapid growth." Information security products catch on in a dramatic way and find an almost insatiable market. IBM jumps into the information security marketplace with both feet, fueling the competitive embers. The national security sector of the government commits fairly substantial sums to research and development. Industry cooperates and the additional R&D produces the technical breakthroughs needed to yield cost-effective, much-enhanced security products. These products find markets not just within the national security side of the government but within large segments of the business community and, to a lesser extent, among the civil sector as well. Industry accepts the demands for a secure environment and products begin to appear that are not clearly COMSEC or COMPUSEC. A major company offers a secure Key Distribution Center, for example. Without a fairly major shift in

government strategy and industry attitudes, this outcome appears unlikely.

Thus, the prospects for an adequate supply of robust security products in the foreseeable future appear dim. Although products, by themselves, are probably not sufficient to achieve information security, they certainly appear to be necessary. Many security regulations and policies are largely useless without the technical mechanisms to enforce them. Personnel and physical security, although helpful in restricting access to an information system, are not particularly helpful in restricting access within it.

We are left, then, with the conclusion that the challenges of information security may well be with us for quite awhile. The technical, legal, social, and moral problems that attend information security are not likely to soon succumb to solution.

But suppose we do succeed? Suppose by some combination of increased commitment, creative energy, and simple good fortune, we discover solutions, at least to most of the technical challenges? Some might argue that our "success" is but a rich source of even greater challenges. They might maintain that our technical solutions have simply unleashed a host of more difficult problems -- problems which involve the power to control -- problems which derive from a seeming paradox between security and secrecy.

Chapter 12

Security vs. Secrecy: In Pursuit of a Balance

In the first chapter of this report, it was suggested that power and restraint are counterpoised. Information one holds constitutes a latent source of power -- not unlike the possession of nuclear weapons in a strategic context. To constitute actual power, there has to be an ability, or at least a perceived ability (and willingness), to make use of the information. In other words, the information must be in a state or condition that permits its use. But, as we have seen, it is exactly this state or condition that places the information in jeopardy and makes it vulnerable. So we are led to protect it. However, to protect against vulnerability almost always imposes restrictions on use, thus limiting the power.

Although this is true, it is not the complete story. As much as power and restraint, viewed from one perspective, act in opposition, when viewed from another, they act to reinforce one another. There is power in restraint, or rather, in the capacity to restrain. The ability to restrain or control is a source of power in and of itself. And it can be the result of power as well.

In her 1982 book Secrets, Sissela Bok writes, "Control over secrecy and openness gives power: it influences what others know, and thus what they choose to do."¹³⁰ The power to protect implies the power not to protect, or to leave unprotected. Thus it is tantamount to the power to exploit. How much of this power U.S. citizens are willing to entrust to their government is uncertain but clearly bounded -- particularly when it extends to their communications or to

information about themselves. Referring to possible government actions to protect private-sector communications, John Metelski writes:

The political and legal risks involved in government action to protect communications might be overcome if the interception problem was of such a demonstrably serious nature that the public, industry, and Congress would accept such heavy-handed government involvement in private-sector telecommunications systems. However, despite Executive and media alarms about the problem, there remains a lack of concern sufficient to support such measures in a programmed, systematic fashion.

Yet without this power to control, any government feels exposed and vulnerable. As Bok puts it:

The conflicts over secrecy may be perennial, but the accelerating pace of technological innovation and the present worldwide political tensions are now unsettling the already precarious standards for keeping, probing, and revealing secrets. New techniques, from ever more sophisticated devices for eavesdropping to computerized data banks, have vastly enlarged the amount of information at the disposal of those with the know-how and the resources to acquire it. This poses extensive threats to individual privacy. It has also made governments and other organizations feel more vulnerable, and increased the felt need for added security [emphasis added]. In the last few years, heightened international tensions have added to the sense of vulnerability -- to fears that plans will be exposed and national security threatened as military, commercial, and scientific secrets are stolen.

The Reagan administration has most certainly given voice to this fear.

But what about this national security argument? Is it true that greater secrecy leads to greater security? The answer is not as clear as it might first appear.

Security, in the sense of well being, seems to derive principally from the absence of fear or anxiety. Although what we know often gives rise to fear, it is usually what we do not know that we fear most. Regardless of the battlefield on which we engage, it is what we do not know about our adversary that usually causes us the greatest concern. Likewise, our adversary, lacking complete information about us, is also

fearful. Former President Carter testifies to this fear and concern when he writes of the arms race between the U.S. and the U.S.S.R.:

A miscalculation or a misunderstanding could be catastrophic, and the excessive desire for secrecy by either nation can be counterproductive because this contributes to suspicion and leads to the taking of countermeasures.¹³³

Some of this anxiety could be ameliorated by better information flow. Tension generally decreases as information flow increases.

Yet it would be naive to accept as total truth that which an adversary -- or even a friend, for that matter -- chooses to dispense to us or lets us have. It seems prudent to "validate" such information with data of our own. Hence, the role of intelligence. Intelligence, when properly used, can relieve tension by providing validation -- completing or filling in the picture that the opponent has painted of himself.

But what about the role of secrecy? Secrecy clearly seeks to impede information flow. If information flow is useful in promoting security in the broader sense, how can secrecy be justified?

There appears to be little problem during wartime. As was noted in Chapter 10, defensive or secrecy measures contributed as significantly as offensive or intelligence successes to the cryptologic advantage enjoyed by the Allies.¹³⁴

Despite its obvious utility, secrecy can also have adverse effects, even in wartime. Gordon Welchman offers this example:

A striking case in point is the Germans' success in taking Crete by airborne assault in May 1941 in spite of the fact that Ultra had revealed every detail of their plans. An inquiry showed that the island need not have been lost if the defending commanders had paid attention to what they were being told. Not knowing the source, however, they had been discounting Ultra messages.¹³⁵

In peacetime, secrecy is even harder to justify. The purpose of secrecy is to deny information. The absence of information contributes to worry, to anxiety, and, in the extreme, to paranoia. Paranoia, in turn, can lead to war. Thus it would seem that secrecy -- the inhibiting of information -- runs a dangerous risk. We recognize this in arms control negotiations when we deliberately provide for mutual verifiability. We create a leak in our own dike. Perhaps during peacetime, the "game" represented by the information war is not zero-sum.

There is another argument that has been raging about secrecy -- one advanced by the "open research" community, especially those engaged in cryptology.¹³⁶ They argue against secrecy in order to obtain a more robust security product -- in other words, to achieve better secrecy. While arguing against secrecy as a means, they seem willing to concede the need for secrecy as an end.

Others, however, argue against secrecy as an end. They argue on the basis of ultimate futility and on the basis of attendant risk. Bok is one of these people. She writes:

While such a response [greater government secrecy] to the growing international tensions and to the greater sense of vulnerability is to some extent understandable, it risks weakening, not strengthening, any nation that adopts it, for it rests on two illusions. The first is that of the efficacy of secrecy given the present level of technological development and of worldwide communication -- the notion that, short of turning an open society into a garrison state, it will be possible to shut down trade, travel, exchange of scientific information, and media and other investigations enough to achieve the desired security. The second illusion is the belief that such secrecy and controls are neutral, that they carry no risks of their own, no danger of damaging creativity, innovation, and research, no barriers to commerce, no dangers to judgment or to character, and no risks of encouraging official negligence and corruption.¹³⁷

The last chapter mentioned the social implications of giving up on the information security problem.¹³⁸ But, there are also social implications associated with solving it -- particularly if that would hand the government greater control over who can know what. Bok writes:

These risks are great when control over secrecy is combined with personal unscrupulousness; greater still when it is joined to unusual political or other power and to special privileges of secrecy such as those granted to professionals; and greatest of all when it is in the hands of government leaders.¹³⁹

In 1980 John Kenneth Galbraith remarked:

One has now the view that the class structure is divided between those who have information and those who do not; those who have access to information and those who must function out of ignorance.¹⁴⁰

And at an international conference in 1979, this statement was made:

"We don't know how real the danger is of a society with a class structure of 'know' and 'know not.'" ¹⁴¹

If the Galbraithian class division existed in 1980, the power to decide the membership of each class did not. Such power, however, would seem to be conferred by the ability to control secrecy.

Yet this power, even if conferred, need not be applied improperly. Lord Acton has been quoted as once having written: "Every thing must degenerate, even the administration of justice" and "Power tends to corrupt, and absolute power corrupts absolutely."¹⁴² But, as Bok points out, Lord Acton "goes too far." She writes:

Every thing secret need not degenerate; some are needed, on the contrary, for growth and creativity. Nor does power always tend to corrupt. It can be exercised with integrity and even tenderness, as in the caring for most infants. A measure of control over secrecy and openness -- and thus of one form of power -- is needed in personal life for equilibrium, liberty, even survival.¹⁴³

Even as individuals need such a "measure of control," so do nations. It has been said that nations at peace might find it difficult to justify secrecy -- that the pursuit of secrecy might be at the risk of the country's own national security. But a nation at peace can soon become a nation at war -- at a time and under circumstances not of its own choice. Without some power to control, any nation would be exceedingly vulnerable. As former CIA Deputy B. R. Inman stated:

The need in today's world for protection of some information, for secrecy, is clear -- I believe -- to any fair observer. Protection of the information necessary to safeguard our society⁴⁴ and to conduct our international affairs, must occur.

Even companies with a large stake in the free flow of information have come to recognize the need for some control. The president of one such company has stated:

For many years my company has been an advocate of the free flow of truthful information. We recognize, however, no freedom can be absolute, and there are reasonable and proper constraints that can and should be placed on the flow of information. So the ideal for the information society might be the orderly flow of truthful information within well-defined boundaries.⁴⁵

After all, the imposition of some controls can permit the relaxing of others. Many forms of protection -- passwords, patents, clearances, copyrights, to name a few -- are sought in order to permit the orderly sharing of information. These forms of protection, in other words, are pursued in order to avoid some of the need for secrecy.

Thus, once again, as has been noted so frequently throughout this paper, it seems that what is called for here is balance. Just as balance is needed when deciding how much centralization can be had without destroying the fragile technical advantages of specialization, and just as balance is required when deciding how much security one can

afford commensurate with the risk, so balance is needed when deciding how much secrecy -- how much ability to control -- is prudent for a democratic government to seek at the cost of reduced liberty for its citizens. Within the constraints of such a balance, the pursuit of security for our nation's information -- however elusive -- is surely in keeping with the highest of moral ideals and worthy of our strongest commitment and greatest effort.

NOTES for Part IV -- Looking Ahead

1. Peter Schweitzer, personal letter to Anthony Oettinger, 26 June 1984.
2. TEMPEST is the name assigned by the government "to investigations and studies of compromising emanations" -- unintentional and frequently revealing radio waves emitted by electronic equipment. (See William J. Broad, "Every Computer 'Whispers' Its Secrets", The New York Times, 5 April 1983, pp. C1, C8).
3. U.S., Department of Defense, National Security Agency, "Industrial Tempest Program (ITP)," a fact sheet dated 1 October 1981.
4. Samuel S. Snyder, "Influence of U.S. Cryptologic Organizations on the Digital Computer Industry," National Security Agency, SRH-003, undated, p. 24.
5. Ibid.
6. Ibid.
7. Samuel S. Snyder, "Computer Advances Pioneered by Cryptologic Organizations," Annals of the History of Computing 2 (January 1980):68.
8. See, for example, Tim Ahern, Associated Press release, Washington dateline section, 27 May 1982.
9. Ray Connolly, "Pentagon to fund major IC program," Electronics, 14 September 1978, p. 81.
10. "VHSIC takes the right direction," Electronics, 22 September 1981, p. 24.
11. Ray Connolly, "The Pentagon goes shopping for technology," Electronics, 30 June 1981, pp. 88ff.
12. Jack Robertson, "Pentagon Awards VHSIC Pacts Worth \$150M-Plus," Electronic News, 4 May 1981, p. 18.
13. Ibid.
14. Above, pp. II-71, 72.
15. J. P. Anderson, "Accelerating Computer Security Innovations," Proceedings of the 1982 Symposium on Security and Privacy (Silver Spring, MD: IEEE Computer Society Press, 1982), p. 91.
16. Above, pp. II-68, II-70 and Note 283 on p. II-109.

17. U.S., Department of Defense Computer Security Center, "Evaluated Products List Summary," CSC-EPL-SUM-84/001.
18. Telephone interview with National Security Agency official, 2 February 1983.
19. Information supplied by Pat Lobeck, ITP Program Manager, National Security Agency.
20. Interview, NSA official.
21. Ibid.
22. This smallness may be an advantage. The NSA source attributes the success of the ITP, in part, to the fact that the entire TEMPEST community is relatively small and the government responsibility is centralized and clearly defined. "You have a small set of people and everybody else is a spectator," he says. "The minute that you get to the point where there is a diffused responsibility [within the government] . . . it would be a lot harder," he adds. (Telephone interview with NSA official).
23. Snyder, "Computer Advances," p. 69.
24. Ibid.
25. Ibid.
26. James Bamford, The Puzzle Palace (Boston: Houghton Mifflin Company, 1982), p. 344.
27. "High Technology: Back in the Bottle?", Technology Review, August/September 1981, p. 77.
28. For a discussion of many of these arguments, see Paul E. Gray, "The University Case Against Secrecy," Technology Review, July 1982, pp. 10-12.
29. Above, p. II-26.
30. Above, p. II-55.
31. Above, pp. II-46 to II-48.
32. Interview with Col. Roger R. Schell, Deputy Director, DoD Computer Security Evaluation Center, National Security Agency, 28 October 1982.
33. See, for example, Don E. Gordon, Electronic Warfare: Element of Strategy and Multiplier of Combat Power (New York: Pergamon Press, 1981), pp. 12, 16-19.
34. Ibid., p. 23.

35. A particular example of the early cryptologic advantage of the Axis side comes from the official history of British Intelligence during World War II. According to this official account, the Germans were enjoying considerable success in breaking both the Administrative Code and the Naval Cypher of the British. When the British switched to their Naval Cypher No. 4, the German rate of success was reduced. Finally, "in June 1943, when the No. 3 and No. 4 books were replaced by Naval Cypher No. 5," the German success against the British Naval Cypher ended altogether. (See F. H. Hinsley, et al., British Intelligence in the Second World War, Vol. II (London: Her Majesty's Stationery Office, 1981), p. 636.)
36. Patrick Beesley, Very Special Intelligence (London: Hamish Hamilton, 1977), p. 33.
37. F. W. Winterbotham, The Ultra Secret (New York: Harper & Row Publishers, 1974), pp. 11, 16-17, 273.
38. Above, p. III-41.
39. Gordon, Electronic Warfare, p. 136.
40. Ibid., p. 139.
41. Science and Government Report, 1 October 1982, p. 5.
42. George I. Davida, "Safety in Numbers," The Sciences, July/August 1981, p. 11.
43. Whitfield Diffie, "NSA and the Independent Cryptographers -- An Uneasy Cooperation," paper distributed by BNR Inc., Mountain View, CA, December 1981, p. 8.
44. Interview with Peter G. Neumann, Assistant Director, Computer Science Laboratory, SRI International, 25 January 1983.
45. Ibid.
46. Telephone interview with James P. Anderson, May 1983.
47. Above, p. II-74.
48. Interview, Schell.
49. Stephen T. Walker, "Introductory Comments," Proceedings of the Fourth Seminar on the DoD Computer Security Initiative, National Bureau of Standards, Gaithersburg, MD, 10-12 August 1981, p. C-2.
50. Anderson, "Accelerating . . . Innovations," p. 95.
51. Ibid., p. 96.
52. Interview, Anderson.

53. Anderson, "Accelerating . . . Innovations," p. 95.
54. William P. King, retiree from the National Security Agency, personal letter to Anthony G. Oettinger, 5 June 1984.
55. Bobby R. Inman, "Keynote Address," Proceedings of the Fourth Seminar on the DoD Computer Security Initiative, National Bureau of Standards, Gaithersburg, MD, 10-12 August 1981, p. B-3.

The disinterest in classified business that Inman here suggests that some manufacturers might have, does indeed exist. See below, pp. IV-32, 33.
56. Above, first Walker quote, p. IV-23.
57. Above, p. II-74.
58. Interview with Admiral Bobby R. Inman, USN (ret.), former Director, National Security Agency, 16 December 1982.
59. Above, pp. III-56 to III-59.
60. James J. Croke, Vice President, Bedford Operations, the MITRE Corporation, personal letter to Anthony G. Oettinger, dated 17 July 1984.
61. Ronald H. Walsh, Senior Manager, Business Development, Systems Development Corporation, A Burroughs Company, personal letter, 21 October 1983.
62. Steven T. Walker, "DoD Perspective on Computer Security," Proceedings of the Fifth Seminar on the DoD Computer Security Initiative, National Bureau of Standards, Gaithersburg, MD, 24-26 May 1982, p. 70.
63. Interview with Steven B. Lipner, Engineering Manager, Security Advanced Development, Digital Equipment Corporation, 3 February 1983.
64. Interview, Neumann.
65. Ibid.
66. Interview with Theodore M. P. Lee, Manager, System Security, Sperry Corporation Computer Systems, 27 April 1983.
67. Based upon a telephone conversation with Lee on 25 May 1983.
68. Theodore M. P. Lee, personal letter, 2 May 1983.
69. Melville H. Klein, "Information Protection in an Information-Intensive Society," Proceedings of the Fifth Seminar on the DoD Computer Security Initiative Program, National Bureau of Standards, Gaithersburg, MD, 24-26 May 1982, p. 57.

70. Above, pp. III-23 to III-25.
71. Interview, Lee.
72. Andrew C. Goldstein, "An Update on Computer Security Activities at Digital," Proceedings of the Fifth Seminar on the DoD Computer Security Initiative, National Bureau of Standards, Gaithersburg, MD, 24-26 May 1982, pp. 241-242.
73. Interview, Lee.
74. Interview with Harry B. DeMaio, Director of Data Security Programs, IBM Corporation, 17 August 1984.
75. Abbott is probably referring here to the portion of the act dealing with accounting standards. This section (91 STAT. 1494, Sec. 102) mandates a "system of internal accounting controls sufficient [among other things] . . . to maintain accountability for assets." This section and its computer security impact are discussed in Rein Turn, Trusted Computer Systems: Needs and Incentives for Use in Government and the Private Sector, The Rand Corporation, Santa Monica, CA, Report R-2811-DR8E, June 1981, pp. 39-40.
76. Robert P. Abbott, "Panel: The Commercial View of Data Security," 1983 IEEE Symposium on Security and Privacy, Oakland, CA, 26 April 1983.
77. Ibid.
78. Leslie S. Chalmers, ibid.
79. Interview, DeMaio.
80. Interview, Lee.
81. Interview, Lipner.
82. Ibid.
83. M. Blake Greenlee, "Financial (Banking) View of Computer Security," Proceedings of the Fifth Seminar on the DoD Computer Security Initiative Program, National Bureau of Standards, Gaithersburg, MD, 24-26 May 1982, p. 168.
84. Ibid.
85. Chalmers, "Panel."
86. Interview, DeMaio.
87. Interview, Lee.

88. U.S., Department of Defense, Computer Security Evaluation Center, Trusted Computer System Evaluation Criteria, Report CSC-STD-001-83, 15 August 1983, p. 57.
89. See U.S., Department of Defense, Computer Security Evaluation Center, Trusted Computer System Evaluation Criteria, Final Draft, 27 January 1983, p. 50.
90. Interview, Neumann.
91. R. Stockton Gaines and Norman Z. Shapiro, "Some Security Principles and their Application to Computer Security," Operating System Review, 12 (July 1978):25.
92. Interview, Neumann.
93. Interview, Lipner.
94. Ibid.
95. Interview, Lee.
96. Interview, Lipner.
97. Ibid.
98. Interview, Lee.
99. Above, p. III-23.
100. Interview with Harold J. Podell, Mission Analysis and Systems Acquisition Division, General Accounting Office, 31 August 1982.
101. This disagreement over appropriate standards has surfaced before in this paper. It was a factor in NSA Director Inman's decision to establish the Computer Security Evaluation Center independent of the existing COMSEC organization. See above, pp. II-82, 83.
102. Interview, Anderson.
103. Ibid.
104. Interview, Lipner.
105. Ibid.
106. From the text of a briefing, "Air Force 2000," reproduced copy, undated.
107. See, for example, Meg Cox, "Network Systems Grows Fast by Finding Ways to Link Different Kinds of Computers," The Wall Street Journal, 6 August 1982, p. 17.

103. Gordon Welchman, The Hut Six Story (New York: McGraw-Hill Book Company, 1982), p. 288.
109. For discussion of the subversion problem, see above, p. III-47. For references to early discussions of most of the other problems, see Note 264 on p. III-107.
110. John Ganty, ed., "Data Encryption: A Pending Necessity," Distributed Processing Newsletter, International Data Corporation, Framingham, MA, Special Report, December 1982, pp. 6-7.
111. George I. Davida, "Safety in Numbers," The Sciences, July/August 1981, p. 9.
112. See, for example, Daniel Bell, "Communications Technology -- for better or for worse," Harvard Business Review, May-June 1979, pp. 20-42.
113. Paul Armer, "Social Implications of the Computer Utility," in Fred Gruenberger, ed., Computers and Communications -- Toward a Computer Utility (Englewood Cliffs, NJ: Prentice-Hall, Inc., 1968), p. 195.
114. See Benjamin M. Compaine, "The New Literacy," Daedalus, Winter 1983, pp. 129-142.
115. Erik Larson, "For Fun or Foul, Computer Hackers Can Crack Any Code," Wall Street Journal, 13 April 1983, pp. 1, 25.
116. Ibid., p. 25.
117. Ibid.
118. Angeline Pantages, "Sophisticated Crime," Dun's Review, August 1979, p. 94.
119. Ibid.
120. Quoted in "A Question of Leadership," Datamation, February 1982, p. 127.
121. Ibid.
122. Above, pp. IV-38, 39.
123. Above, pp. IV-36.
124. Interview with John P. L. Woodward, Group Leader, Computer and Networking Technology, The MITRE Corporation, 11 August 1982.
125. Interview, Neumann.
126. Quoted in "A Question of Leadership," Datamation, February

- 1983, p. 120.
127. Interview, Neumann.
128. Ibid.
129. U.S., General Accounting Office, Federal Information Systems Remain Highly Vulnerable to Fraudulent, Wasteful, Abusive and Illegal Practices (MASAD-82-18), 21 April 1982, p. 25.
130. Sissela Bok, Secrets (New York: Pantheon Books, 1982), p. 282.
131. John Metelski, "Telecommunications privacy and the information society," Telecommunications Policy, December 1978, p. 329.
132. Bok, Secrets, p. 284.
133. Jimmy Carter, Keeping Faith: Memoirs of a President (New York: Bantam Books, 1982), p. 249.
134. Above, pp. IV-16 to IV-18.
135. Welchman, Hut Six Story, p. 279.
136. See, for example, George I. Davida, "The Case Against Restraints on Non-Governmental Research in Cryptography," Cryptologia, July 1981, pp. 143-148.
137. Bok, Secrets, p. 285.
138. Above, pp. IV-51, 52.
139. Bok, Secrets, p. 282.
140. John Kenneth Galbraith, from remarks during The Information Society: A Transcript of a Sixty Minutes Documentary, Aspen Institute for Humanistic Studies, 1980, p. 16.
141. Martyn F. Roetter and Malcolm H. Ross, "Is 'Small' Necessarily Beautiful?" Teleinformatics '79, E. J. Boutmy and A. Danthine (ed.), (Amsterdam: North-Holland Publishing Company, 1979), p. 267.
142. Quoted in Bok, Secrets, p. 105.
143. Ibid., pp. 105-106.
144. B. R. Inman, "National Security and Technical Information," speech to the American Association for the Advancement of Science, Washington, D.C., 7 January 1982.
145. J. V. White, "Privacy in the Information Society," Vital Speeches, 1 March 1982, p. 314. (J. V. White is the president of Equifax, Inc.)

APPENDICES

A PLAN FOR
THE EVALUATION OF
TRUSTED* COMPUTER SYSTEMS

SUMMARY

This document describes a plan for the establishment of a Federal Computer Security Evaluation Center. The purpose of this Center is to 1) establish standards of integrity for trusted* computer systems, 2) conduct evaluations of industry and government developed computer systems for compliance with these standards and 3) assist government agencies in the proper use of trusted computer systems within their information system operations. The Center will be located at the National Bureau of Standards in Gaithersburg, MD and will be supported jointly by the Departments of Commerce (DoC) and Defense (DoD) and the Intelligence Community (IC).

The establishment of a Federal Computer Security Evaluation Center, providing consistent technical evaluations of the integrity of computer systems for use throughout the Federal government is essential. The ability to trust the integrity of computer systems is of great significance throughout the Federal government, including but not limited to the DoD and Intelligence Communities. Trusted computer systems able to serve the broad information system needs of the Federal government and private industry are now being developed by the private sector computer manufacturing industry as part of their normal system development process. The government must establish an efficient and consistent mechanism for evaluating the integrity of computer systems in order to be able to make full use of these trusted systems. While the sensitive information handling requirements of different parts of the government vary widely, the technical evaluation of the integrity of a computer system is the same regardless of the end use of the system. The Federal Computer Security Evaluation Center will perform this technical evaluation process and make the results available throughout the Federal government.

* A trusted computer is one which employs sufficient hardware and software integrity measures to allow its use for simultaneously processing multiple levels of classified and/or sensitive information.

FUNCTIONS of the COMPUTER SECURITY EVALUATION CENTER

The Computer Security Evaluation Center shall:

1. Establish and maintain technical criteria for the evaluation of the integrity of computer systems.
2. Conduct evaluations of industry and government developed computer systems against these technical criteria.
3. Establish procedures to insure the proper maintenance and distribution of trusted computer systems.
4. Advise government organizations on the proper use of trusted computer systems within the total context of their sensitive information handling requirements.
5. Promote the understanding of the essential elements of trusted computer system development and use through interdepartmental cooperative efforts and public seminars and workshops.
6. Provide direct assistance on a limited basis for specific government trusted system information handling developments.
7. Coordinate federal government research in the development and use of trusted computer systems.
8. Sponsor research activities in the development of trusted computer system evaluation procedures and techniques.

EVALUATION PROCESS

The sensitivity of the information processed by computers and the environments in which information handling systems operate varies widely. There are systems both in the Defense community and throughout the government that operate on very sensitive information in highly constrained environments, while other systems operate on information considered only slightly sensitive in unconstrained environments. There are systems which process classified information, proprietary information, information considered sensitive for privacy reasons, and financial and logistics information. There is also a growing desire in many communities to allow access to a single system or a network of systems by users with different access rights in order to improve the effectiveness of the overall organization. The degree of protection required for these systems varies with the sensitivity of the information and the constraints on the environment in which they operate.

As shown by recent computer security research efforts, there are many technical measures which influence the degree of integrity which one can place in the hardware /software of a computer system. There are system design and implementation measures which when properly used will yield a computer system with a high degree of internal integrity. Many new computer systems are being developed using these techniques. Many older computer systems, while not employing these techniques, still possess reasonable integrity provisions by virtue of the use of good design practices, careful implementation and rigorous testing. There are also many existing systems which have no significant internal integrity measures and can only be used in environments where no reliance is placed on the integrity of the hardware or software.

Not all environments in which computers will operate on sensitive information will require the same level of integrity within the computer system. When the user community is trusted because of extensive background investigations, leaving only a need to know requirement, and the physical protection against external penetration is high, systems with relatively strong integrity but not employing rigorous assurance measures may be suitable. When the sensitivity of the information is relatively low and there is a reasonable degree of physical protection, these same systems may be suitable. When the sensitivity of the data is high and there is a spectrum of users with different access rights using the system, the requirement

The Center will establish technical evaluation criteria which will be used to evaluate trusted systems.

Evaluations of industry or government developed systems will be conducted by the Center upon request by the developer of the system. The evaluation will be performed on a mutually beneficial basis with no binding obligations on either party. The system developer, in submitting a system for evaluation, is under no obligation to complete its development or to market the system. The government, in agreeing to undertake the evaluation of a system, assumes no obligation to complete the evaluation or to purchase any version of the product at any time. If during the evaluation, either the system developer or the government should conclude that they cannot continue the evaluation, the effort will be terminated by suitable notification of the other party. It is the intent of the government to perform these evaluations to enhance its ability to determine suitable environments/applications for trusted systems and it is assumed that the system developers will submit systems which they intend to make available on a general basis.

The primary concern of the Center will be the evaluation of general purpose trusted computer systems which are now or will soon be available for use anywhere in the federal government. Systems which are of limited general utility or of a highly specialized nature will not be evaluated by the Center except by special arrangement. The Center will provide advice to responsible authorities throughout the federal government on establishing proper evaluation procedures for specialized systems.

The evaluation process which the Center will conduct will determine, based on technical features present in a computer system and the assurance procedures used to guarantee that those features work correctly, the environments for which a particular system may be suitable. The evaluation process has been evolving over the past two years and has been refined to a series of integrity classes as shown in the Evaluated Products List (EPL), Figure 1.1. The concept of an EPL is an established procurement mechanism which allows the evaluation of a product prior to any procurement actions and the use of the evaluation results in any future requests for proposal (RFP) in lieu of having to repeat the evaluation for each RFP.

For higher degrees of system design and implementation verification will be necessary.

EVALUATED PRODUCTS LIST

<u>CLASS</u>	<u>TECHNICAL FEATURES</u>	<u>EXAMPLES</u>	<u>POSSIBLE ENVIRONMENTS</u>
1	—	MOST COMMERCIAL SYSTEMS	DEDICATED MODE
2	FUNCTIONAL SPECIFICATION REASONABLE PENETRATION RESULTS	"MATURE" "ENHANCED" OPERATING SYSTEM	BENIGN, NEED TO KNOW ENVIRONMENTS
3	REASONABLE MODERN PROGRAMMING TECHNIQUES LIMITED SYSTEM INTEGRITY MEASURES	MULTICS	AF DATA SERVICE CENTER TS-S
4	FORMAL DESIGN SPECIFICATIONS SYSTEM INTEGRITY MEASURES		NO USER PROGRAMMING TS-S-C
5	PROVEN DESIGN SPECIFICATIONS VERIFIABLE IMPLEMENTATION LIMITED COVERT PATH PROVISIONS	KSOS KVM	LIMITED USER PROGRAMMING TS-S-C
6	VERIFIED IMPLEMENTATION AUTOMATED TEST GENERATION EXTENDED COVERT PATH PROVISIONS REASONABLE DENIAL OF SERVICE PROVISIONS		FULL USER PROGRAMMING TS-S-C

The results of these evaluations will be made available to federal government organizations responsible for establishing security policy for their communities. The Center will also advise these groups as to appropriate environments/ applications for which evaluated systems may be suitable. The Center's responsibility is to establish and maintain the technical evaluation criteria and to conduct technical evaluations. The final determination of policy as to the suitability of particular classes of systems for use in particular environments /applications is the responsibility of the security policy organization for each particular federal community.

Evaluation reports will consist of at least two parts: a public report summarizing the integrity status of the system and the environments/ applications recommended as suitable, and a detailed report (or reports) describing the evaluation process and any specific vulnerabilities which remain within the evaluated system. Portions of this second report will generally be both classified and proprietary to the system developer. It will be necessary for the developer to have a cleared facility and technical personnel to be able to participate fully in the Center's vulnerability analyses. If a developer cannot establish such a facility, it will be necessary to properly sanitize the vulnerability analysis report prior to making it available to the developer.

The evaluation criteria will include a series of technical protection measures and the necessary procedures for assuring that they work correctly. The greater the combination of mechanisms and assurance procedures, the greater the confidence that can be placed in the integrity of the system and the more sensitive the environments and applications for which the system will be suitable. Included in the assessment of suitable environment/ applications for a particular class of systems will be recommended additional physical, administrative and procedural security measures to insure the total system integrity.

TRUSTED SYSTEM DISTRIBUTION

Once a computer system has been evaluated, care must be exercised to insure that the trusted portion of the system is distributed using proper procedures. A master copy of the evaluated system will be maintained by the Center at all times for comparison purposes. Distribution will whenever possible be the responsibility of the

developer's cleared system control officer using procedures established and approved by the Center.

SYSTEM DEVELOPER'S RESPONSIBILITIES

The system developer, upon entering an evaluation agreement with the Center, will be requested to supply detailed design and implementation information on the trusted portions of the computer system being evaluated. The evaluation can be performed only on the basis of the information supplied; lack of detailed information will result in lower confidence in the integrity of the system.

Under the best of circumstances, the system developer will have a fully cleared development staff associated with the design and implementation of the new product. This situation is not expected to be generally available but the system developer should have a cleared system control facility in order to be able to participate fully in the integrity vulnerability analysis and to provide for system distribution. If the system developer cannot maintain a cleared system control facility, this may limit the degree of trust that can be placed in the system. In this case, special provisions will be needed to insure suitable system distribution.

In the process of conducting an evaluation, the Center must be able to duplicate any integrity assurance measures which may be employed in the system's development. It will be necessary for the developer to supply the Center with background information on the integrity assurance measures employed in developing the system in order for the Center to adequately evaluate these assurance procedures.

EVALUATION CENTER

The Federal Computer Security Evaluation Center will be a joint program of the Departments of Commerce and Defense and will receive funds and personnel from both organizations. The Director of the Center will be an employee of the National Bureau of Standards. The technical staff will consist of NES employees and assignees from the military services and defense agencies as well as other Federal government organizations. The support staff and all administrative functions will be

provided by NES.

The Center will perform the evaluation of general purpose trusted computer systems as part of its basic responsibilities. Advise to government agencies on the use of the results of these evaluations will also be provided as a basic responsibility. Specialized evaluations unique to one system or organization and detailed technical advise on a specialized project will be provided on a cost reimbursable basis. The Center will interact with designated system evaluation groups within a Department or Agency rather than with specific system developers except under special arrangements. Each Department or Agency will be encouraged to establish a system evaluation group for detailed interactions with their specific system developers.

The initial Center staff will consist of approximately twelve technical personnel and three support staff. All members of the staff must hold Top Secret clearances or be clearable to Top Secret. A limited number of the staff should also have sufficient intelligence community clearances to ensure effective interaction on specialized community needs. The Center must have facilities for handling classified information at least through Secret and proprietary information from multiple sources. Center personnel must have liberal travel provisions because the technical evaluation process will require considerable travel to system developer's facilities.

The Center must have the ability to contract for support of its evaluation efforts. There must be provision for use of technical consultants from industry and the academic community for specialized analyses and the development of industry wide standards. The Center must develop a set of system evaluation tools including penetration aids, and system specification and program verification tools. The Center must develop the capability to understand the integrity assurance measures which the system developers will be using in their product development efforts. This capability must include the ability to completely duplicate any integrity assurance measures that a developer employs. In general the developer will be required to supply complete design and implementation information about the product including whatever integrity assurance measures have been employed. The Center will validate those measures including full repeat of the procedures when necessary.



THE DEPUTY SECRETARY OF DEFENSE

WASHINGTON, D.C. 20301

JAN 2 1981

MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN, JOINT CHIEFS OF STAFF
DIRECTOR, DEFENSE ADVANCED RESEARCH
PROJECTS AGENCY
DIRECTOR, DEFENSE COMMUNICATIONS AGENCY
DIRECTOR, DEFENSE INTELLIGENCE AGENCY
DIRECTOR, DEFENSE INVESTIGATIVE SERVICE
DIRECTOR, DEFENSE LOGISTICS AGENCY
DIRECTOR, DEFENSE MAPPING AGENCY
DIRECTOR, DEFENSE NUCLEAR AGENCY
DIRECTOR, NATIONAL SECURITY AGENCY
DIRECTOR, WWMCC SYSTEM ENGINEERING

SUBJECT: DOD Computer Security Evaluation Center

Although your comments in response to Dr. Dinneen's memorandum of November 15 indicate some concern about working relationships within the proposed Evaluation Center, there is no disagreement or doubt regarding the need. Therefore, the proposal made by the Director, National Security Agency to establish a Project Management Office is approved. Effective January 1, 1981, the Director, National Security Agency is assigned the responsibility for Computer Security Evaluation for the Department of Defense.

Please provide the name of your representative for computer security matters to ASD(C³I). The individual chosen for this task should be empowered to work in your behalf to develop and coordinate the charter and implementing directives for the Center. I expect this working group to identify necessary personnel and fiscal resources.

W. Graham Claytor, Jr.

cc: ASD(C³I)
ASD(Comptroller)
DUSD(Policy Review)

34344



October 25, 1982

NUMBER 5215.1

Department of Defense Directive

SUBJECT: Computer Security Evaluation Center

References: (a) DoD Directive 5200.28, "Security Requirements for Automatic Data Processing (ADP) Systems," December 18, 1972
(b) DoD 5200.28-M, "ADP Security Manual," January 1973, authorized by reference (a)
(c) OMB Circular No. A-71, Transmittal Memorandum No. 1, "Security of Federal Automated Information Systems," July 27, 1978
(d) through (m), see enclosure 1

A. PURPOSE

This Directive establishes the DoD Computer Security Evaluation Center (CSEC), provides policy, and assigns responsibilities for the technical evaluation of computer system and network security, and related technical research.

B. APPLICABILITY AND SCOPE

1. This Directive applies to the Office of the Secretary of Defense (OSD), the Military Departments, the Organization of the Joint Chiefs of Staff, the Unified and Specified Commands, and the Defense Agencies (hereafter referred to as "DoD Components").

2. Its provisions govern the conduct of trusted computer system evaluation and technical research activities within the Department of Defense in support of overall computer system security evaluation and approval responsibilities assigned to the DoD Components under references (a), (b), (c), DoD Directives 5220.22, and 5400.11 (references (d) and (e)).

C. DEFINITIONS

1. Sensitive/Classified Information. Sensitive information as defined in reference (c), and classified information as defined in DoD 5200.1-R (reference (f)).

2. A Trusted Computer System. Employs sufficient hardware and software integrity measures to allow its use for processing simultaneously a range of sensitive or classified information.

3. Generic Computer Security Research and Development. Has potential application over a very broad, generalized basis, and includes experimental exploration and development of feasible and potentially useful technology, responsive to a broad class of computer security needs.

D. POLICY

1. It is DoD policy to encourage the easy availability of trusted computer systems. The establishment of the DoD CSEC, the consolidation of generic computer security research and development (R&D), the evaluation of computer security systems and the establishment of an Evaluated Products List (EPL) are designed to further this objective.

2. The DoD Consolidated Computer Security Program (CCSP) shall include resources for the operation of the CSEC and for generic computer security R&D activities in support of DoD Components. The DoD Components are responsible for DoD Component security research, development, test, and evaluation (RDT&E) efforts and application-dependent research and development for specific DoD Component systems.

3. The activities and products of the CSEC, including technical advice and support, shall complement the established responsibilities of DoD Components relating to the overall policy, security evaluation, and approval of computer systems as prescribed in DoD Directive 5200.28, DoD 5200.28-M, OMB Circular A-71, Directives 5220.22 and 5400.11 (references (a), (b), (c), (d), and (e)), for the processing, use, and production of sensitive and classified information.

4. The EPL is not intended to replace prescribed procurement practices in the acquisition of computers and computer services. The CSEC and EPL are established to assist procuring activities in evaluating available products; computer products or services will not be rejected on the basis that the product or service is not on an EPL.

E. PROCEDURES

Procedures for consolidated technical research are at enclosure 2.

F. RESPONSIBILITIES

1. The Under Secretary of Defense for Research and Engineering (USDR&E), or his designee, shall:

a. Provide overall policy direction, guidance, and management oversight for the CSEC in coordination with the Deputy Under Secretary of Defense (Policy) (DUSD(P)) and the Assistant Secretary of Defense (Comptroller) (ASD(C)).

b. Establish a steering committee composed of representatives of DoD Components to review center activities and recommend future directions.

c. In coordination with the Deputy Assistant Secretary of Defense (Policy) (DUSD(P)) and the Assistant Secretary of Defense (Comptroller) (ASD(C)) represent the Secretary of Defense with other government agencies, foreign

governments, the North Atlantic Treaty Organization (NATO), and to the extent permitted, industry, in trusted computer system evaluation policy matters. Enter into agreements, if appropriate, consistent with National Disclosure Policy (reference (g)), with other government agencies, foreign governments, and NATO.

d. Establish an information exchange forum on computer security matters among DoD Components.

2. The Director, National Security Agency (NSA), in cooperation with the USDR&E, shall:

a. Establish and operate the CSEC as a separate and unique entity within the NSA.

b. Program and budget for CCSP support resources under procedures prescribed for the DoD planning, programing, and budgeting processes, but excluding National Foreign Intelligence Program funds controlled by the Director of Central Intelligence (DCI) under E.O. 12333 (reference (h)).

c. Appoint a Director to manage the CSEC who shall:

(1) Establish and maintain technical standards and criteria for the evaluation of trusted computer systems that can be incorporated readily into the DoD Component life-cycle management process (DoD Directives 7920.1, 5000.29, 5000.1, 5000.2 (references (i),(k),(l),(m))). Provide assistance to the DoD Components in the application of the technical standards and criteria.

(2) Conduct evaluations of selected industry and government-developed trusted computer systems against these criteria. Request for evaluation of government-developed computer systems will be from the DoD Component responsible for the security of the system to be evaluated.

(3) Maintain and publish an EPL of the selected industry and government-developed trusted computer systems that is suitable for use by the DoD Components.

(4) Conduct and sponsor R&D for trusted computer systems, and for computer security evaluation and verification methods and techniques.

(5) Provide assistance to the DoD Components by conducting evaluations of selected DoD and DoD contractor trusted computer systems in response to requests from the DoD Component responsible for the security of the computer system to be evaluated.

(6) Serve as the focal point for technical matters concerning the use of trusted computer systems for the protection of sensitive and classified information and, in conjunction with DoD Component computer security test and evaluation activities, provide technical advice to the DoD Components.

(7) Sponsor DoD Component cooperative efforts, public seminars, and workshops for the purpose of technology transfer.

Oct 25, 82
5215.1

(8) Serve as the DoD principal technical point of contact on trusted computer system matters with other government agencies, industry, foreign governments, and NATO under the policy guidance of the USDR&E or designee, consistent with National Disclosure Policy (reference (g)).

(9) Develop and maintain the CCSP, in conjunction with DoD Components. (See procedures at enclosure 2).

3. Heads of DoD Components, or designees, shall:

a. Make maximum use of the standards, technical criteria, and evaluations promulgated by the CSEC in meeting their responsibilities for overall automatic data processing (ADP) system security evaluation, approval, and maintenance as set forth in DoD Directive 5200.28, DoD 5200.28-M, DoD Directives 5220.22, and 5400.11 (references (a), (b), (d), and (e)).

b. Establish overall ADP security policy for specific types of sensitive and classified information under their security cognizance, and prescribe the security procedures and constraints appropriate for the classes of trusted computer systems as defined in the EPL.

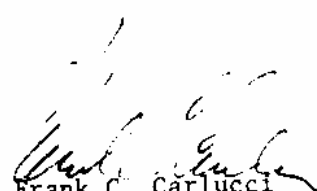
c. Designate central DoD Component focal points for interaction with the CSEC in the development of Component trusted computer systems.

d. Formulate jointly the CCSP and manage directly the execution of their respective portions of the CCSP in accordance with enclosure 2.

e. Conduct RDT&E to meet specific operational needs identified by Component requirements.

G. EFFECTIVE DATE AND IMPLEMENTATION

This Directive is effective immediately. Forward two copies of implementing document to the Under Secretary of Defense for Research and Engineering within 120 days.


Frank C. Carlucci
Deputy Secretary of Defense

Enclosures - 2

1. References
2. Summary of Procedures for Consolidated Technical Research

REFERENCES, continued

- (d) DoD Directive 5220.22, "DoD Industrial Security Program," December 8, 1980
- (e) DoD Directive 5400.11, "Department of Defense Privacy Program," June 9, 1982
- (f) DoD 5200.1-R, "Information Security Program Regulation," August 1982, authorized by DoD Directive 5200.1, "DoD Information Security Program," June 7, 1982
- (g) DoD Instruction 5230.17, "Procedures and Standards for Disclosure of Military Information to Foreign Activities," August 17, 1979
- (h) Executive Order 12333, "United States Intelligence Activities" December 4, 1981
- (i) DoD Directive 7920.1, "Life Cycle Management of Automated Information Systems (AIS)," October 17, 1978
- (j) DoD Directive 7200.1, "Administrative Control of Appropriations," November 15, 1978
- (k) DoD Directive 5000.29, "Management of Computer Resources in Major Defense Systems," April 26, 1976
- (l) DoD Directive 5000.1, "Major Systems Acquisition," March 9, 1982
- (m) DoD Directive 5000.2, "Major Systems Acquisition Process," March 19, 1980

PROCEDURES FOR CONSOLIDATED TECHNICAL RESEARCH

This establishes the procedures for developing the generic computer security R&D portion of the CCSP, as defined in subsection C.3. of this Directive. Portions of the CCSP relating solely to the operations of the CSEC are not included in this summary.

1. Under paragraph F.2.b. of this Directive, the Director, NSA, shall issue a data call for each fiscal year to the DoD Components for the CCSP. The data call shall request identification of major tasks and milestones for that fiscal year.

2. DoD Components shall submit to NSA their proposed projects for generic computer security R&D in the format prescribed. This shall include a program-quality technical description, cost estimates, and recommendation for the execution responsibility, namely, the submitting Component, another Component, or the CSEC. The CSEC similarly shall prepare its own proposals.

3. The CSEC shall convene the technical review group (TRG) composed of an identified principal from each DoD Component with participation by the working level engineering, scientific, communications and data processing personnel of DoD Components and the CSEC. The purpose and function of this group is to review the Component submissions for redundancies, completeness, and resource requirements, and to determine initial priorities. The TRG deliberations are directed toward an understanding and agreement among all principals of the nature and scope of the proposed CCSP research and development projects.

4. The CSEC shall compile the TRG-reviewed projects and provide the DoD Components a copy of the draft program for review and comment.

5. The Director, CSEC, shall chair the program working group (PWG) which is composed of a principal from each DoD Component. The function of the PWG is to review and refine the priorities for the generic security R&D portion of the CCSP under published OSD guidance. The PWG shall recommend the generic computer security R&D program to the Director, NSA. The CSEC shall prepare the draft consolidated computer security R&D program and provide the Components a copy for review and comment.

6. The Director, NSA, shall chair the program manager's review group (PMRG) consisting of representatives from DoD Components, including the Deputy Assistant Secretary of Defense (Communications, Command, Control, and Intelligence) and the Deputy Assistant Secretary of Defense (Research and Advanced Technology) as members, with additional observers, as appropriate. A formal briefing on the overall CCSP shall be presented to the Director and this group.

7. The Director, NSA, shall approve the CCSP after considering the changes or modifications suggested by this review group. This shall constitute the basis for the CCSP portion of the NSA Program Objectives Memorandum (POM) submission.

8. Acting upon published guidance and based on the approved CCSP, NSA shall make the budget submission for the CCSP. The CSEC shall distribute the CCSP portion of the NSA POM submission to the DoD Components.

9. Before anticipated appropriation, the PWG shall refine further priorities, confirm execution responsibilities, and identify possible candidates in the event of program reductions. These actions shall be the basis for sub-allocation of funding.

10. Following receipt of obligational authority, NSA shall suballocate CCSP funds to DoD Components for their approved tasks under DoD Directive 7200.1 (reference (j)). The suballocation process requires that each DoD Component provide to NSA by the 15th of each month a status report of commitments and obligations of the CCSP funds.

THE WHITE HOUSE

WASHINGTON

September 17, 1984

*National Security
Decision Directive 145
(Unclassified Version)*

NATIONAL POLICY ON TELECOMMUNICATIONS
AND AUTOMATED INFORMATION SYSTEMS SECURITY

Recent advances in microelectronics technology have stimulated an unprecedented growth in the supply of telecommunications and information processing services within the government and throughout the private sector. As new technologies have been applied, traditional distinctions between telecommunications and automated information systems have begun to disappear. Although this trend promises greatly improved efficiency and effectiveness, it also poses significant security challenges. Telecommunications and automated information processing systems are highly susceptible to interception, unauthorized electronic access, and related forms of technical exploitation, as well as other dimensions of the hostile intelligence threat. The technology to exploit these electronic systems is widespread and is used extensively by foreign nations and can be employed, as well, by terrorist groups and criminal elements. Government systems as well as those which process the private or proprietary information of US persons and businesses can become targets for foreign exploitation.

Within the government these systems process and communicate classified national security information and other sensitive information concerning the vital interests of the United States. Such information, even if unclassified in isolation, often can reveal highly classified and other sensitive information when taken in aggregate. The compromise of this information, especially to hostile intelligence services, does serious damage to the United States and its national security interests. A comprehensive and coordinated approach must be taken to protect the government's telecommunications and automated information systems against current and projected threats. This approach must include mechanisms for formulating policy, for overseeing systems security resources programs, and for coordinating and executing technical activities.

This Directive: Provides initial objectives, policies, and an organizational structure to guide the conduct of national activities directed toward safeguarding systems which process or communicate sensitive information from hostile exploitation; establishes a mechanism for policy development; and assigns

responsibilities for implementation. It is intended to assure full participation and cooperation among the various existing centers of technical expertise throughout the Executive Branch, to promote a coherent and coordinated defense against the hostile intelligence threat to these systems, and to foster an appropriate partnership between government and the private sector in attaining these goals. This Directive specifically recognizes the special requirements for protection of intelligence sources and methods. It is intended that the mechanisms established by this Directive will initially focus on those automated information systems which are connected to telecommunications transmission systems.

1. Objectives. Security is a vital element of the operational effectiveness of the national security activities of the government and of military combat readiness. Assuring the security of telecommunications and automated information systems which process and communicate classified national security information, and other sensitive government national security information, and offering assistance in the protection of certain private sector information are key national responsibilities. I, therefore, direct that the government's capabilities for securing telecommunications and automated information systems against technical exploitation threats be maintained or improved to provide for:

a. A reliable and continuing capability to assess threats and vulnerabilities, and to implement appropriate, effective countermeasures.

b. A superior technical base within the government to achieve this security, and support for a superior technical base within the private sector in areas which complement and enhance government capabilities.

c. A more effective application of government resources and encouragement of private sector security initiatives.

d. Support and enhancement of other policy objectives for national telecommunications and automated information systems.

2. Policies. In support of these objectives, the following policies are established:

a. Systems which generate, store, process, transfer or communicate classified information in electrical form shall be secured by such means as are necessary to prevent compromise or exploitation.

b. Systems handling other sensitive, but unclassified, government or government-derived information, the loss of which could adversely affect the national security interest,

shall be protected in proportion to the threat of exploitation and the associated potential damage to the national security.

c. The government shall encourage, advise, and, where appropriate, assist the private sector to: identify systems which handle sensitive non-government information, the loss of which could adversely affect the national security; determine the threat to, and vulnerability of, these systems; and formulate strategies and measures for providing protection in proportion to the threat of exploitation and the associated potential damage. Information and advice from the perspective of the private sector will be sought with respect to implementation of this policy. In cases where implementation of security measures to non-governmental systems would be in the national security interest, the private sector shall be encouraged, advised, and, where appropriate, assisted in undertaking the application of such measures.

d. Efforts and programs begun under PD-24 which support these policies shall be continued.

3. Implementation. This Directive establishes a senior level steering group; an interagency group at the operating level; an executive agent and a national manager to implement these objectives and policies.

4. Systems Security Steering Group.

a. A Systems Security Steering Group consisting of the Secretary of State, the Secretary of the Treasury, the Secretary of Defense, the Attorney General, the Director of the Office of Management and Budget, the Director of Central Intelligence, and chaired by the Assistant to the President for National Security Affairs is established. The Steering Group shall:

(1) Oversee this Directive and ensure its implementation. It shall provide guidance to the Executive Agent and through him to the National Manager with respect to the activities undertaken to implement this Directive.

(2) Monitor the activities of the operating level National Telecommunications and Information Systems Security Committee and provide guidance for its activities in accordance with the objectives and policies contained in this Directive.

(3) Review and evaluate the security status of those telecommunications and automated information systems that handle classified or sensitive government or government-derived information with respect to established objectives and priorities, and report findings and recommendations through the National Security Council to the President.

(4) Review consolidated resources program and budget proposals for telecommunications systems security, including the COMSEC Resources Program, for the US Government and provide recommendations to OMB for the normal budget review process.

(5) Review in aggregate the program and budget proposals for the security of automated information systems of the departments and agencies of the government.

(6) Review and approve matters referred to it by the Executive Agent in fulfilling the responsibilities outlined in paragraph 6. below.

(7) On matters pertaining to the protection of intelligence sources and methods be guided by the policies of the Director of Central Intelligence.

(8) Interact with the Steering Group on National Security Telecommunications to ensure that the objectives and policies of this Directive and NSDD-97, National Security Telecommunications Policy, are addressed in a coordinated manner.

(9) Recommend for Presidential approval additions or revisions to this Directive as national interests may require.

(10) Identify categories of sensitive non-government information, the loss of which could adversely affect the national security interest, and recommend steps to protect such information.

b. The National Manager for Telecommunications and Information Systems Security shall function as executive secretary to the Steering Group.

5. The National Telecommunications and Information Systems Security Committee.

a. The National Telecommunications and Information Systems Security Committee (NTISSC) is established to operate under the direction of the Steering Group to consider technical matters and develop operating policies as necessary to implement the provisions of this Directive. The Committee shall be chaired by the Assistant Secretary of Defense (Command, Control, Communications and Intelligence) and shall be composed of a voting representative of each member of the Steering Group and of each of the following:

The Secretary of Commerce
The Secretary of Transportation
The Secretary of Energy

Chairman, Joint Chiefs of Staff
 Administrator, General Services Administration
 Director, Federal Bureau of Investigation
 Director, Federal Emergency Management Agency
 The Chief of Staff, United States Army
 The Chief of Naval Operations
 The Chief of Staff, United States Air Force
 Commandant, United States Marine Corps
 Director, Defense Intelligence Agency
 Director, National Security Agency
 Manager, National Communications System

b. The Committee shall:

(1) Develop such specific operating policies, objectives, and priorities as may be required to implement this Directive.

(2) Provide telecommunication and automated information systems security guidance to the departments and agencies of the government.

(3) Submit annually to the Steering Group an evaluation of the status of national telecommunications and automated information systems security with respect to established objectives and priorities.

(4) Identify systems which handle sensitive, non-government information, the loss and exploitation of which could adversely affect the national security interest, for the purpose of encouraging, advising and, where appropriate, assisting the private sector in applying security measures.

(5) Approve the release of sensitive systems technical security material, information, and techniques to foreign governments or international organizations with the concurrence of the Director of Central Intelligence for those activities which he manages.

(6) Establish and maintain a national system for promulgating the operating policies, directives, and guidance which may be issued pursuant to this Directive.

(7) Establish permanent and temporary subcommittees as necessary to discharge its responsibilities.

(8) Make recommendations to the Steering Group on Committee membership and establish criteria and procedures for permanent observers from other departments or agencies affected by specific matters under deliberation, who may attend meetings upon invitation of the Chairman.

(9) Interact with the National Communications System Committee of Principals established by Executive Order

12472 to ensure the coordinated execution of assigned responsibilities.

c. The Committee shall have two subcommittees, one focusing on telecommunications security and one focusing on automated information systems security. The two subcommittees shall interact closely and any recommendations concerning implementation of protective measures shall combine and coordinate both areas where appropriate, while considering any differences in the level of maturity of the technologies to support such implementation. However, the level of maturity of one technology shall not impede implementation in other areas which are deemed feasible and important.

d. The Committee shall have a permanent secretariat composed of personnel of the National Security Agency and such other personnel from departments and agencies represented on the Committee as are requested by the Chairman. The National Security Agency shall provide facilities and support as required. Other departments and agencies shall provide facilities and support as requested by the Chairman.

6. The Executive Agent of the Government for Telecommunications and Information Systems Security. The Secretary of Defense is the Executive Agent of the Government for Communications Security under authority of Executive Order 12333. By authority of this Directive he shall serve an expanded role as Executive Agent of the Government for Telecommunications and Automated Information Systems Security and shall be responsible for implementing, under his signature, the policies developed by the NTISSC. In this capacity he shall act in accordance with policies and procedures established by the Steering Group and the NTISSC to:

a. Ensure the development, in conjunction with NTISSC member departments and agencies, of plans and programs to fulfill the objectives of this Directive, including the development of necessary security architectures.

b. Procure for and provide to departments and agencies of the government and, where appropriate, to private institutions (including government contractors) and foreign governments, technical security material, other technical assistance, and other related services of common concern, as required to accomplish the objectives of this Directive.

c. Approve and provide minimum security standards and doctrine, consistent with provisions of the Directive.

d. Conduct, approve, or endorse research and development of techniques and equipment for telecommunications and automated information systems security for national security information.

e. Operate, or coordinate the efforts of, government technical centers related to telecommunications and automated information systems security.

f. Review and assess for the Steering Group the proposed telecommunications systems security programs and budgets for the departments and agencies of the government for each fiscal year and recommend alternatives, where appropriate. The views of all affected departments and agencies shall be fully expressed to the Steering Group.

g. Review for the Steering Group the aggregated automated information systems security program and budget recommendations of the departments and agencies of the US Government for each fiscal year.

7. The National Manager for Telecommunications Security and Automated Information Systems Security. The Director, National Security Agency is designated the National Manager for Telecommunications and Automated Information Systems Security and is responsible to the Secretary of Defense as Executive Agent for carrying out the foregoing responsibilities. In fulfilling these responsibilities the National Manager shall have authority in the name of the Executive Agent to:

a. Examine government telecommunications systems and automated information systems and evaluate their vulnerability to hostile interception and exploitation. Any such activities, including those involving monitoring of official telecommunications, shall be conducted in strict compliance with law, Executive Orders and applicable Presidential Directives. No monitoring shall be performed without advising the heads of the agencies, departments, or services concerned.

b. Act as the government focal point for cryptography, telecommunications systems security, and automated information systems security.

c. Conduct, approve, or endorse research and development of techniques and equipment for telecommunications and automated information systems security for national security information.

d. Review and approve all standards, techniques, systems and equipments for telecommunications and automated information systems security.

e. Conduct foreign communications security liaison, including agreements with foreign governments and with international and private organizations for telecommunications and automated information systems security, except for those foreign intelligence relationships conducted for intelligence purposes by the Director of Central Intelligence. Agreements shall be coordinated with affected departments and agencies.

f. Operate such printing and fabrication facilities as may be required to perform critical functions related to the provision of cryptographic and other technical security material or services.

g. Assess the overall security posture and disseminate information on hostile threats to telecommunications and automated information systems security.

h. Operate a central technical center to evaluate and certify the security of telecommunications systems and automated information systems.

i. Prescribe the minimum standards, methods and procedures for protecting cryptographic and other sensitive technical security material, techniques, and information.

j. Review and assess annually the telecommunications systems security programs and budgets of the departments and agencies of the government, and recommend alternatives, where appropriate, for the Executive Agent and the Steering Group.

k. Review annually the aggregated automated information systems security program and budget recommendations of the departments and agencies of the US Government for the Executive Agent and the Steering Group.

l. Request from the heads of departments and agencies such information and technical support as may be needed to discharge the responsibilities assigned herein.

m. Enter into agreements for the procurement of technical security material and other equipment, and their provision to government agencies and, where appropriate, to private organizations, including government contractors, and foreign governments.

8. The Heads of Federal Departments and Agencies shall:

a. Be responsible for achieving and maintaining a secure posture for telecommunications and automated information systems within their departments or agencies.

b. Ensure that the policies, standards and doctrines issued pursuant to this Directive are implemented within their departments or agencies.

c. Provide to the Systems Security Steering Group, the NTISSC, Executive Agent, and the National Manager, as appropriate, such information as may be required to discharge responsibilities assigned herein, consistent with relevant law, Executive Order, and Presidential Directives.

9. Additional Responsibilities.

a. The Secretary of Commerce, through the Director, National Bureau of Standards, shall issue for public use such Federal Information Processing Standards for the security of information in automated information systems as the Steering Group may approve. The Manager, National Communications System, through the Administrator, General Services Administration, shall develop and issue for public use such Federal Telecommunications Standards for the security of information in telecommunications systems as the National Manager may approve. Such standards, while legally applicable only to Federal Departments and Agencies, shall be structured to facilitate their adoption as voluntary American National Standards as a means of encouraging their use by the private sector.

b. The Director, Office of Management and Budget, shall:

(1) Specify data to be provided during the annual budget review by the departments and agencies on programs and budgets relating to telecommunications systems security and automated information systems security of the departments and agencies of the government.

(2) Consolidate and provide such data to the National Manager via the Executive Agent.

(3) Review for consistency with this Directive, and amend as appropriate, OMB Circular A-71 (Transmittal Memorandum No. 1), OMB Circular A-76, as amended, and other OMB policies and regulations which may pertain to the subject matter herein.

10. Nothing in this Directive:

a. Alters the existing authorities of the Director of Central Intelligence, including his responsibility to act as Executive Agent of the Government for technical security countermeasures (TSCM).

b. Provides the NTISSC, the Executive Agent, or the National Manager authority to examine the facilities of other departments and agencies without approval of the head of such department or agency, nor to request or collect information concerning their operation for any purpose not provided for herein.

c. Amends or contravenes the provisions of existing law, Executive Orders, or Presidential Directives which pertain to the privacy aspects or financial management of automated information systems or to the administrative requirements for safeguarding such resources against fraud, abuse, and waste.

d. Is intended to establish additional review processes for the procurement of automated information processing systems.

11. For the purposes of this Directive, the following terms shall have the meanings indicated:

a. Telecommunications means the preparation, transmission, communication or related processing of information by electrical, electromagnetic, electromechanical, or electro-optical means.

b. Automated Information Systems means systems which create, prepare, or manipulate information in electronic form for purposes other than telecommunication, and includes computers, word processing systems, other electronic information handling systems, and associated equipment.

c. Telecommunications and Automated Information Systems Security means protection afforded to telecommunications and automated information systems, in order to prevent exploitation through interception, unauthorized electronic access, or related technical intelligence threats, and to ensure authenticity. Such protection results from the application of security measures (including cryptosecurity, transmission security, emission security, and computer security) to systems which generate, store, process, transfer, or communicate information of use to an adversary, and also includes the physical protection of sensitive technical security material and sensitive technical security information.

d. Technical security material means equipment, components, devices, and associated documentation or other media which pertain to cryptography, or to the securing of telecommunications and automated information systems.

12. The functions of the Interagency Group for Telecommunications Protection and the National Communications Security Committee (NCSC) as established under PD-24 are subsumed by the Systems Security Steering Group and the NTISSC, respectively. The policies established under the authority of the Interagency Group or the NCSC, which have not been superseded by this Directive, shall remain in effect until modified or rescinded by the Steering Group or the NTISSC, respectively.

13. Except for ongoing telecommunications protection activities mandated by and pursuant to PD/NSC-24, that Directive is hereby superseded and cancelled.

4
3
2
1

1
2
3
4