If you have issues viewing or accessing this file contact us at NCJRS.gov.

[COMMITTEE PRINT]

COMPUTER AND COMMUNICATIONS SECURITY AND PRIVACY

REPORT

PREPARED BY THE

SUBCOMMITTEE ON
TRANSPORTATION, AVIATION AND MATERIALS

TRANSMITTED TO THE

COMMITTEE ON
SCIENCE AND TECHNOLOGY
U.S. HOUSE OF REPRESENTATIVES

NINETY-EIGHTH CONGRESS

SECOND SESSION

Serial AA

APRIL 1984

95323

For the use of the Committee on Science and Technology

U.S. GOVERNMENT PRINTING OFFICE
WASHINGTON : 1984

COMMITTEE ON SCIENCE AND TECHNOLOGY

DON FUQUA, Florida, *Chairman*

ROBERT A. ROE, New Jersey
GEORGE E. BROWN, JR., California
JAMES H. SCHEUER, New York
RICHARD L. OTTINGER, New York
TOM HARKIN, Iowa
MARILYN LLOYD, Tennessee
DOUG WALGREN, Pennsylvania
DAN GLICKMAN, Kansas
ALBERT GORE, JR., Tennessee
ROBERT A. YOUNG, Missouri
HAROLD L. VOLKMER, Missouri
BILL NELSON, Florida
STAN LUNDINE, New York
RALPH M. HALL, Texas
DAVE McCURDY, Oklahoma
MERVYN M. DYMALLY, California
PAUL SIMON, Illinois
NORMAN Y. MINETA, California
RICHARD J. DURBIN, Illinois
MICHAEL A. ANDREWS, Texas
BUDDY MacKAY, Florida
TIM VALENTINE, North Carolina
HARRY M. REID, Nevada
ROBERT G. TORRICELLI, New Jersey
FREDERICK C. BOUCHER, Virginia
LARRY WINN, JR., Kansas
MANUEL LUJAN, JR., New Mexico
ROBERT S. WALKER, Pennsylvania
WILLIAM CARNEY, New York
F. JAMES SENSENBRENNER, JR., Wisconsin
JUDD GREGG, New Hampshire
RAYMOND J. McGRATH, New York
JOE SKEEN, New Mexico
CLAUDINE SCHNEIDER, Rhode Island
BILL LOWERY, California
ROD CHANDLER, Washington
HERBERT H. BATEMAN, Virginia
SHERWOOD L. BOEHLERT, New York
ALFRED A. (AL) McCANDLESS, California
TOM LEWIS, Florida

HAROLD P. HANSON, *Executive Director*
ROBERT C. KETCHAM, *General Counsel*
REGINA A. DAVIS, *Chief Clerk*
DAVID S. JEFFERY, *Minority Staff Director*

SUBCOMMITTEE ON TRANSPORTATION, AVIATION AND MATERIALS

DAN GLICKMAN, Kansas, *Chairman*

ALBERT GORE, JR., Tennessee
MERVYN M. DYMALLY, California
RICHARD L. OTTINGER, New York
TOM HARKIN, Iowa
MICHAEL A. ANDREWS, Texas
WILLIAM CARNEY, New York
SHERWOOD L. BOEHLERT, New York
ALFRED A. (AL) McCANDLESS, California

LETTER OF SUBMITTAL

HOUSE OF REPRESENTATIVES,
COMMITTEE ON SCIENCE AND TECHNOLOGY,
Washington, D.C., April 1984.

Hon. DON FUQUA,
Chairman, Committee on Science and Technology,
U.S. House of Representatives.

DEAR MR. CHAIRMAN: It is my pleasure to present to you the Subcommittee's report on Computer and Communications Security and Privacy. It is based on hearings before the Subcommittee last September 26 and October 17 and 24.

The report centers on the immense growth of computer usage by government, business, private organizations and individuals; the ramifications of that growth; and ways to cope with the potential dangers of those ramifications.

The problems and potential problems range from hackers who have outwitted large corporations and government agencies by tapping into their computers, to criminals who can master the capability of making illegal international bank transfers. Electronic intrusion can give private medical information to total strangers, disrupt air traffic control systems, and endanger national security. The potential for abuse and misuse of computers is very serious indeed.

The Subcommittee recommendations call for a national commission to examine comprehensively a vast array of multi-jurisdictional issues that arise from consideration of this subject. These include the vulnerability of critical national computer systems, computer crime, the effect of new technologies on personal privacy and the Federal role in protecting information on citizens.

I would especially like to thank Mrs. Louise Becker of the Congressional Research Service for her many valuable contributions to both the hearings and the preparation of this report.

With best regards,

Sincerely,

DAN GLICKMAN,
Chairman, Subcommittee on Transportation,
Aviation and Materials.

U.S. Department of Justice
National Institute of Justice

This document has been reproduced exactly as received from the person or organization originating it. Points of view or opinions stated in this document are those of the authors and do not necessarily represent the official position or policies of the National Institute of Justice.

Permission to reproduce this ~~copyrighted~~ material has been granted by

Public Domain/
U.S. House of Representatives

to the National Criminal Justice Reference Service (NCJRS).

Further reproduction outside of the NCJRS system requires permission of the ~~copyright~~ owner.

CONTENTS

Chapter I. Findings and Recommendations

A. National Commission

Finding

Computer and communications systems are key to the functioning of virtually every institution of modern society. Government, commerce and industry have all welcomed this technological change, often without fully understanding that it was taking place. Furthermore, few have appreciated either the extent of our dependence or the national consequences when such systems fail or are misused. Information systems and processes along with the data contained within them represent assets of incalculable value to their owners and to the society at large. Intentional and unintentional threats and vulnerabilities of these resources are real and therefore present a problem of national significance.

The aspects of this subject include an array of multifaceted issues including national security and defense, vulnerability of critical systems (e.g. financial institutions, electric power generation, telephone systems, air traffic control, and industrial processes), the effect of technology on privacy, computer-related crime, and the social and political consequences of intensive computerization. However, because of the complexity and multijurisdictional character of these issues, it is unlikely that any single Executive Branch organization or Congressional Committee will be able to deal effectively with all of them.

Recommendation

Congress should charter a national commission to examine the vast set of interrelated issues surrounding the security and privacy of computer/communications systems, especially those that transcend either the jurisdictional boundaries of Federal, state and local government agencies or public and private sector interests. After a thorough examination of the problems, the Commission should outline a framework for policy and guidance of future Federal Government actions.

The Commission should:

Examine the legal, economic, institutional, social and technical aspects of safeguarding computerized resources.

Study the scope and nature of threats and vulnerabilities of computer/communications systems.

Assume a broad perspective to include national security and defense, privacy and confidentiality, computer crime and abuse, vulnerabilities of critical national systems, and the implications of technological innovation on government, society and the individual.

Address the merits and disadvantages of possible legal, technical and administrative remedies to protect national computer/communications systems from intrusion and abuse.

B. FEDERAL LEADERSHIP

Finding

The Federal Government has a role in protecting computer/communications systems of national importance as well as those that are needed to support operations of Federal agencies. Traditionally, the Federal role has been limited to securing systems associated with national defense and intelligence activities; however, there is growing concern that both public and private sector critical systems such as banking, utilities, entitlement systems, law enforcement and industrial processes need additional protection.

Lack of Federal leadership is evident from the fact that there is inadequate central focus to deal with computer/communications security. There has not been a concentrated effort to identify problems nor strengthen computer/communications security programs. Historically, the Office of Management and Budget (OMB) has not conducted follow-up reviews nor overseen risk assessment efforts as required by its own procedures. It has failed to develop new directives to meet recent developments and has not encouraged the other central management agencies (General Services Administration, National Bureau of Standards, Office of Personnel Management) to develop a strong set of directives to assist Federal agencies in establishing computer/communications security programs.

Recommendation

The Administration should begin an immediate assessment of the problems and issues in order to develop a set of national policies that will ensure the protection of critical national systems relevant to government, industry, commerce, and the society. Specific attention should be given to protecting against unauthorized intrusion into critical systems. To this end, the Administration is urged to view computer and communications security in the broadest possible perspective to include the legal, economic, institutional, social and technical aspects.

Responsibility for national critical systems should be pinpointed and the appropriate controls implemented. The Administration should establish a central focus with wide agency participation (national security, defense, intelligence, law enforcement, emergency management, commerce, etc.) to ensure that all facets of computer security are addressed. The Administration should review related policies and guidance documents to improve and strengthen Federal and national programs related to computer/communications security. In addition the Administration should begin a review and oversight of Federal systems security with a view toward enhancing such systems so that they may serve as a model for nationally critical systems.

The Federal Government should play a more active role in raising computer/communications security awareness in the private sector. It should develop an "early warning" system to examine

and alert the public to possible problems with new applications of information technology (e.g. electronic mail).

C. TECHNICAL AND ADMINISTRATIVE GUIDANCE TO FEDERAL AGENCIES

Finding

There is no clear focus for technical and administrative direction of Federal agencies. Agencies are not always clear as to what steps to take to appropriately secure their computer/communications systems. The lack of an appropriate set of security directions and guidelines, especially in non-national defense areas, creates confusion and chaos in the way government computers are run. This could result in disruption of vital services such as air traffic control and federal funds transfer.

Recommendation

The Office of Management and Budget should establish a central focus to provide technical assistance to agencies that are responsible for sensitive, non-national security data in selecting tools and techniques to protect their computer systems. Such a focus could, for example, be created by expanding the role of the DOD Computer Security Center or by creating a civil entity patterned after it. Furthermore, the General Services Administration should consider developing a manual to provide agencies with administrative guidance in planning, developing and implementing computer security measures.

D. RESEARCH AND DEVELOPMENT

Finding

There is a need for effective and low cost computer/communication safeguards. Countermeasures are sometimes deemed too costly and system managers are reluctant to invest in technologies which may hamper systems performance or limit systems use. Appropriate technological protective measures do not exist for all applications; therefore, there is a need to promote research and development of security technologies with lower cost and greater efficiency.

Recommendation

Existing resources within the computer security community (vendors, computer security experts, etc.) and the Federal Government should be channeled to pursue expanded research efforts to improve computer/communication security. At the Federal level the Administration should encourage the DOD Computer Security Center and the National Bureau of Standards (NBS) Institute for Computer Science and Technology (ICST) to identify vulnerabilities which may affect future systems and support relevant security research.

The National Science Foundation (NSF), in collaboration with the DOD Center and NBS, should begin to identify the critical areas that might benefit from additional research efforts. The National Science Foundation should plan to increase support of basic

research on computer security, including human factors essential to improving the security of an automated information system.

The private sector should be encouraged to identify where research is needed to improve computer/communication security. In addition, incentives to encourage private sector research in both technological and administrative safeguards should be developed. Consideration should be given to establishing a central focus to identify countermeasures research which has the broadest application.

Responsibilities for computer communication/security research should be clear and Federal direction should be well established to prevent duplication. Coordination and joint efforts between private sector and Government as well as among Government agencies should be strengthened.

A permanent Federal task force, consisting of both management and mission agencies, should be established to provide direction and coordination of Federal computer-communication security research efforts.

E. THREATS AND VULNERABILITIES

Finding

Although media attention consistently focuses on the threats from "computer hackers" and other outside intruders, the greatest threat to computerized resources remains personnel who are authorized to access them.

Recommendation

The Administration should strengthen clearance procedures for Federal workers handling sensitive, non-national security data. All Federal workers handling sensitive, non-national security data should be certified and receive awareness training on computer abuse, including penalties for unwanted (illegal) activites.

All Federal automated information systems and related documentation should contain an explicit warning or notification regarding unlawful activities or abuses.

The private sector should be encouraged to consider developing an employee clearance/certification program and a notification system for warning that abuses and unlawful activities will be punished.

F. CERTIFICATION OF SYSTEMS

Finding

Computer/communication systems depend on devices and techniques to provide an appropriate level of security. The operation and functioning of these devices are not always fully understood and users are rarely able to test their accuracy or durability. In addition, since some may be systems or environment dependent—that is, their function may differ from one system to another—a careful assessment should be made to certify their reliability and validity. Both private and public sectors need tested products. Consequently, there is a need for a certification of hardware (equipment) and software (computer programs) to determine their adequacy in providing the appropriate level of security.

Recommendation

The private sector should be encouraged to develop a certification process (e.g. underwriters laboratories) and a voluntary standards program to give users information on the specific capability of a device or technique as well as to indicate the condition or environment that permits optimum functioning.

The Federal Government should encourage agencies to select proven products and devices based on the requirements and specific environment. The DOD Computer Security Center list of evaluated products should be expanded so that it may be useful in systems which process sensitive non-defense data (e.g. tax and financial information, medical, and personal).

G. TRAINING AND SECURITY AWARENESS

Finding

Training and education represent a foundation for improving the security of computer/communications systems. Unsophisticated manpower can lead to poor planning, design, implementation, and monitoring of security aspects of automated computer/communication systems. There is a shortage of capable and well-trained computer security personnel. The lack of skilled computer/communication security manpower not only affects systems design and operation but makes it difficult to detect abuses and threats to these systems. The lack of trained criminal justice officials limits detection and successful prosecution of cases involving computer crime and abuse.

Recommendation

Both public and private sector organizations should expand the training of existing manpower to improve their computer security programs. This training should not be limited to technical personnel but should also include managers, users and operators so that all personnel associated with information systems will understand their role in protecting computers, communication networks, and data.

Federal training programs should be developed so that all government systems can draw on certified specialists to safeguard computerized resources. Specifically, the Office of Personnel Management (OPM) should develop an in-depth training program aimed at improving specific skills associated with computer security. OPM should create a special classification for computer/communication security specialists and prescribe the requirements for each class of specialist.

Universities and institutions of higher learning should expand programs so that a sufficient number of skilled individuals will be available to plan, design, and develop both systems and security technologies, including self-diagnostic tools, secure operating systems and other devices.

The National Science Foundation should identify elements which would enhance the computer security aspect of university comput-

er science programs. In addition, NSF should consider enhancing support for those computer scientists pursuing programs which have a strong computer/communication security orientation.

There should be increased support and expanded training of Federal criminal justice officials to detect and prosecute computer-related crimes. The Federal Bureau of Investigation Academy computer crime program should be expanded so that a greater number of criminal justice officials will receive training.

H. NON-NATIONAL SECURITY DATA CLASSIFICATION

Finding

The defense and national security communities use a prescribed and defined classification scheme (confidential, secret, top secret) to designate the sensitivity of data. This scheme ultimately provides the basis for selecting the appropriate level of protection required for handling and accessing the data. Knowing the sensitivity of the data allows the effective selection of computer and communication security tools and techniques. Organizations which do not have a hierarchical data scheme to designate the sensitivity of data sometimes find it difficult to select appropriate safeguards.

The DOD Computer Security Center's "evaluation criteria" is responsive to the national security classification scheme. The Center's partnership with industry and its aim to encourage the broad use of its "evaluation criteria" and research-supported products suggests establishing a hierarchical classification scheme for non-national security data. Such a scheme might include designations such as "non sensitive", "sensitive" and "sensitive critical".

Recommendation

The Office of Management and Budget should consider the advantages of establishing a non-national security data classification scheme to protect certain categories of sensitive data (e.g. financial, medical, inventory systems, etc.) in the Federal Government. OMB should undertake an independent survey to assess the experience of other organizations in using such classification schemes.

The DOD Computer Security Center, in conjunction with the private sector, should undertake to identify private sector use of data classification schemes. The Center should assess the value of these schemes in relationship to the Center's Evaluation Criteria.

I. COMPUTER ABUSE REPORTING

Finding

The lack of reliable statistics on computer/communications systems abuses contributes to a misunderstanding of the problem and hampers implementation of adequate safeguards.

Recommendation

The Administration should develop uniform standards for identifying and reporting computer crimes and abuses. A center of responsibility for Federal computer crime and abuse reporting should be established.

CHAPTER II. BACKGROUND

Computers and communications systems permeate many aspects of a modern society. Because of the importance of the information in these systems, the increased reliance on information technologies, and the large dollar investment in data, equipment, and software, the need to protect these resources is growing. These factors, according to the hearing record, prompted the Committee on Science and Technology, Subcommittee on Transportation, Aviation and Materials, chaired by Representative Dan Glickman, to examine some of the critical issues related to computer and communications security and privacy. The subcommittee conducted three days of hearings on September 26, October 17, and 24, 1983.[1] The subcommittee's investigation focused on:

The adequacy of our national policies to cope with unwanted intrusions into computer/communications systems;

The effect on personal privacy from abuse and misuse of information systems;

The implications and dimensions of computer security research and development; and

The appropriate role of Government in protecting critical computer/communications systems.

A. UNDERSTANDING THE ISSUES

Information technologies, supportive communication networks, and data are key to a wide spectrum of activities in both the public and private sector. Safeguarding these resources is essential to the nation, the government, and the individual.

The Federal Government spends approximately $12 billion annually on automatic data processing and telecommunications equipment.[2] While this figure relates only to equipment (hardware), nevertheless it is indicative of the enormous investment being made to support automated information systems. Furthermore, it is projected by the General Services Administration (GSA) that by the end of the 1980s the Federal Government will have an inventory of about 25,000 medium- to large-scale computers and some 500,000 micro-computers. Government is not alone in investing in computerization of records and information. The private sector also has an enormous investment in modern information technology and a continued interest in using it for varied applications. This continuous growth and dependence on information technology stimulates interest in the adequacy of protective measures to prevent unauthorized disclosure, unwarranted manipulation, and destruction of these resources.

---

[1] The following review and analysis derives from U.S. Congress. House. Committee on Science and Technology. Subcommittee on Transportation, Aviation and Materials. Computer and Communications Security and Privacy, 98th Cong., 1st Sess., Hearings held Sept. 26, Oct. 17, and 24, 1983. Washington, U.S. Govt. Print. Off., 1983. 546 p.
Hereafter referred to as Hearing.
For a general discussion of computer and communications security and privacy, see U.S. Library of Congress. Congressional Research Service. Computer Security: An Overview of National Concerns and Challenges. Feb. 3, 1983. Authored by Louise Giovane Becker. Washington, 1983. Multilith no. 83-135. 241 p. Hereafter referred to as Computer Security: An Overview of National Concerns and Challenges.

[2] Hearings. Ibid., p. 106.

Computer/communications security encompasses a wide range of activities associated with the life-cycle management of automated information resources and telecommunication networks. These activities attempt to assure that computers/communications are maintained with adequate confidentiality, accuracy, integrity, and availability to achieve desired goals and objectives of the organizations.[3]

Traditionally the national security and defense communities have provided leadership and support for computer/communications security research. More recently non-defense agencies and the private sector have come to realize that there are dangers confronting unprotected systems and sensitive data (financial, personal data, proprietary information, etc.), and that adequate safeguards must be provided.[4]

Media reports of unauthorized access of Government and non-Government computer/communications systems by a group of young "computer hackers," who referred to themselves as the "414s", recently called attention to the vulnerability of some systems. Over the years incidents of computer-assisted crimes, sabotage of computer/communications facilities, and misuse of the technology and information have highlighted the need to curtail abuses. In addition, intentional and unintentional actions which result in errors, interruption of services, unwanted access to and manipulation of data, damage to equipment and information, hardware or software weaknesses, and failure in support systems (power or air conditioning) cause additional concerns. The potential harm to computer resources from natural disasters, espionage, wiretapping and interception of emanations (electromagnetic radiation), further increases concern.

Organizations often find protecting computer/communications systems difficult. Part of the problem is that they often fail to allocate adequate resources and to order priorities effectively. Some organizations are reluctant to make the necessary investment in a computer security program; others find that even after they identify problems, economic and efficient security tools are not available. Since computer/communications security often requires a mixture of physical, technical, and administrative security measures, each organization must select the appropriate safeguards carefully.

The related computer/communications security issues are complicated by a myriad of technical factors. Some of the issues are related to national security and defense, computer crime and abuse, privacy and confidentiality, and international data exchanges.

Dr. Willis Ware of the Rand Corporation, a leading computer security expert, testifying before the House Subcommittee on Transportation, Aviation, and Materials on October 24, 1983 distinguished between security and privacy. He said:

> Let me first clarify the relationship between security and privacy, where I use the latter term in the context of record-keeping privacy, namely the use of information about people to make decisions and judgments about them.

[3] Computer Security: An Overview of National Concerns and Challenges, Ibid., p. 1.
[4] Ibid., p. 2.

> Record-keeping privacy concerns personal information kept in computer based systems, and the essence of it is protecting such information and controlling its use for authorized purposes. In contrast, computer security is that body of technology, techniques, procedures, and practices that provides the protective mechanisms to assure the safety of both the computer systems themselves and the information within them; and in addition, limits access to such information solely to authorized users. Computer security is of importance whether the information to be protected is personal in nature and therefore relative to privacy; whether it is defense in nature and therefore related to the security of the country; or whether it is sensitive in nature and therefore relevant to corporate welfare in the private sector. The important point to be noted is that a comprehensive set of security safeguards within and around a computer-based information system is an essential prerequisite for assuring personal privacy. To operate such a system without relevant safeguards is a sham against privacy assurance.[5]

Dr. Ware cautioned that:

> The computer security issue must be seen as analogous to the classical offense/defense situation. As computer security safeguards become stronger, the offenses against them will become more sophisticated and the cycle will repeat. Therefore, no organization or Congress can assume that the computer security issue is one that can be looked at and forgotten. It first surfaced on the professional scene only fifteen years ago; we are still low on the learning curve with regard to knowing how to incorporate comprehensive protection mechanisms in our systems. It is an evolving issue, not a static end-of-the-road one to be dismissed.[6]

Mr. Elmer Clegg of Honeywell Information Systems, Inc., testifying at the same hearings, expanded on the scope of computer security. In discussing the dimensions of the remedies, he commented that:

> Computer security is a multi-faceted discipline which requires the use of hardware, software, and operational procedures to provide protection of valuable resources. The extent of these mechanisms depends on the value of the information versus the cost of its unauthorized disclosure.[7]

Mr. Clegg explained that:

> Protection of a computer system requires a complete program of (1) Procedural Security, (2) Physical Security, (3) Communications Security, and (4) Operating Systems Security.[8]

[5] Hearing, Ibid., p. 455-456.
[6] Ibid.
[7] Ibid., p. 530.
[8] Ibid., p. 530-531.

Procedural Security requires formal methods for controlling access to classified or sensitive information. These protection methods are often the enforcement of regulation, as in the Department of Defense, or of audit principles as in industry.

Physical Security addresses the protection within the physical environment of the computer facility. The protection of the computer from physical attack has received a great deal of attention since the 60s when bombing computer centers was a form of protest. Today computers are protected by security systems such as sophisticated burglar/fire alarms, guards, card keys, and other physical protection devices and techniques.

Communications Security is addressed through the use of encryption and protection against electromagnetic emanation from transmission lines. The use of the Data Encryption Standard (DES) and Tempest approved equipment is the most well known method of providing communications security.

Operating Systems Security is the system of internal controls in the computer which ensure that all data in the system are protected from unauthorized access or disclosure as well as from tampering. The DoD Computer Security Center [Discussed in Detail Below] has developed criteria which define the features and techniques necessary to provide operating systems security at various risk levels.

B. NATIONAL CONCERNS

Among the many critical and sensitive computer/communications systems which contribute to the national welfare, are those supporting electronic funds transfer, entitlement programs, medical care, law enforcement, and air traffic control systems. Since computer/communications security measures are not uniformly applied, these systems are vulnerable to abuse and misuse. Early in the subcommittee's examination it became apparent that systems handling national security classified data are associated with a stringent set of controls while other systems did not always receive similar levels of protection. In addition, Federal agencies handling unclassified data tend to view security problems in a narrow context and they often fail to approach computer security management comprehensively. For example, documentation on security processes may be non-existent, or limited, or personnel clearance for trustworthiness may not be required. Another set of problems affecting such systems stems from the lack of a central focus dedicated to identifying problems and addressing concerns. The lack of clear direction often hampers Federal agencies and other organizations from instituting appropriate remedies.

C. SCOPE OF THE HEARINGS

Congress continues to have an interest in enhancing and improving computerized resources, especially those of national interest. Over the years Congress has enacted laws to protect certain data. For example, the Privacy Act of 1974 and the Omnibus Crime Control and Safe Streets Act, have stimulated implementation of computer security measures. Other Federal statutes require that confidentiality of census data, social security information, and the individual's tax return be maintained. In addition, both Public Law 89-306 (Brooks Act) and the Paperwork Reduction Act of 1980 call for improved management of information technologies. Nevertheless, the subject of protecting computerized resources is often approached from a narrow perspective. For this reason, the subcommittee structured the hearings to provide a broadly based perspective on this multifaceted topic.

The subcommittee's hearings specifically focused on the following:

What are the current and future threats to and vulnerabilities of a society dependent on computer/communications resources;

What is the present scope of computer/communications security research efforts;

What is the extent of Federal and private sector involvement in improving computer security;

What legal, social, and economic changes are needed to safeguard computerized resources;

What is the role of key Federal agencies in providing computer/communications security direction (policy formulation, resources allocation, and ordering priorities); and

How can the Federal Government encourage research on computer/communications safeguards and encourage implementation of the appropriate protective measures?

The witnesses testifying at the subcommittee's hearings included computer security experts, representatives of Government agencies, and the private sector. (See Appendix A for a complete listing.) Both technical and administrative problems were outlined. In addition, witnesses identified specific issues that might require special consideration. While the intent of the subcommittee hearing provided a perspective on some of the problems, the complexity of the topics did not allow a complete review of all the issues. In a number of instances witnesses identified other issues which may require further consideration by Congress and others. Specifically there may be need for additional review and oversight of the following issues:

Implication of new information technologies on security and privacy;

Balancing national security requirements and private sector needs;

Identifying policy direction with regard to international data exchanges (transborder data flows);

Improving computer/communications security research and development; and

Evaluating the advantages and problems of instituting a classification scheme for non-national security data handled by Federal agencies.

CHAPTER III. SUMMARY AND ANALYSIS OF THE HEARINGS

A. INTRODUCTION

This section identifies issues and concerns raised at the subcommittee's three days of hearings on computer/communications systems security and privacy.

At the first of the three hearings, discussion focused on key problems affecting automated information resources and related technologies. Witnesses at the hearing included a young "computer hacker" associated with the "414s" and several private sector computer security experts. The second day of hearings highlighted Federal Government computer/communications security activities. Government witnesses from the Office of Management and Budget, General Accounting Office, DOD Computer Security Center, Federal Bureau of Investigation, National Bureau of Standards, and Department of the Treasury identified the Government's approach to improving computer/communications security. On the third day of hearings, testimony was received from representatives of the private sector, including expert witnesses from the financial community and industry. (See Appendix A for the list of witnesses.) At the beginning of the three day hearings the chairman of the subcommittee, Representative Dan Glickman highlighted the growing dependence on information technology: [9]

> Computers and the communications links that connect them are becomming more and more important to modern society. Banks, hospitals, schools, business of all kinds, and the military have assembled vast amounts of data on which they, and we, depend. In fact, the average citizen is probably unaware of the true extent that computers touch his daily life. Because computers are usually unseen, few of us, I suspect, are fully aware of their growth and importance.

Given the importance of these critical systems, the Chairman expressed concern that these systems were not always adequately protected. He cautioned that "in some cases, we have failed to take the most elementary precautions, the electronic equivalent of locking the door." [10]

B. SOME GENERAL PROBLEMS AND POSSIBLE REMEDIES

The concerns identified at the hearing encompassed a broad range of legal, technical, administrative, and social issues. This section discusses the following topics: protection of personal privacy; threats and vulnerabilities, such as personnel, computer hackers, poor password controls; and the implications of certain technical innovations. Also discussed were possible counter-measures and potential solutions.

Mr. Jimmy McClary, Division Leader for Operational Security and Safeguards Division of Los Almos National Laboratroy in his testimony highlighted some of the key problems which affect the

[9] Ibid., p. 1.
[10] Ibid.

entire computer security community. Specifically he mentioned that: [11]

> First, there are not enough people with the proper expertise and training in computer security. Programs to develop such individuals are badly needed.
>
> Second, better low-cost methods for identifying computer users are needed. The password systems in use today are vulnerable to attacks based on lost or stolen passwords and do not provide us with sufficient confidence that users can be accurately identified. On the other hand, systems that can provide us with greater confidence are too costly for most applications.
>
> Third, a much wider use of encryption would make a major improvement in security of computing systems. The development of inexpensive encryption devices would lead to systems which are more secure than those currently in use.
>
> Finally, we need a realistic attitude toward those who abuse information processing systems. Obtaining unauthorized access to a government or private sector computer is not a game. At best it is a willful act little different from a joyride in a stolen car.

Chairman Glickman expressed amazement that it is not possible to determine if systems are being intentionally jeopardized or sabotaged.[12]

Mr. McClary offered the following insight into the problem.[13]

> Two of the biggest problems in computer security right now are software and hardware verification. That is, software verification is the question of, is the program I'm running really the one that I wrote and expected to execute. That's an extremely difficult problem, one that's well worth solving if we can. That's the problem you're talking about, the problem of determining that the program you are running is the one that you think you're running that no one has added something to it or changed something. It is not a simple problem.

He went on to say:

> Nor is there hardware verification . . . verifying that someone hasn't come in and modified your hardware.

Another concern raised at the hearing is that with the proliferation of computers and the increased number of people knowledgeable about computer systems operations, it becomes increasingly difficult to control access. A leading computer expert, Mr. Donn Parker of SRI International, identified three basic aspects of computer know how; namely, "skill," "access," and "information" which may provide the basis for greater vulnerability. Mr. Parker stated that "with the ever increasing number of computer systems,

[11] Ibid., p. 37–38.
[12] Ibid., p. 49.
[13] Ibid.

both personal and mainframe alike, information and skill is spreading to an ever-increasing number of individuals and institutions." [14] He went on to predict that in the not too distant future with higher stakes, increased levels of knowledge and other aspects better understood, there will be a trend toward more, higher technological level systems penetrations and circumvention.[15] This, Mr. Parker believes, will make it harder "to deter and detect" computer abuses.

Witnesses at the hearing expressed concern with the imbalance between what is being spent on hardware and software versus what is being dedicated to protecting these systems. The problems have been exacerbated by groups such as the computer hackers, who are drawn to penetrate systems and who are motivated not only by possible gain but the mere challenge of doing it. Witnesses alluded to this trend as the equivalent of automobile "joy riding". They cautioned that this phenomena has grave consequences for the future since predictably more individuals will have the skills to access a greater number of computer resources. (See part 2 b. for discussion of the "computer hacker".)

Richard Shriver, Assistant Secretary of the Treasury, Electronic Systems and Information Technology, summarized the potential threats to the Department of the Treasury as follows:

> Those attempting to improperly divert Government funds;
>
> Those attempting to gain improper access to sensitive financial information;
>
> Those attempting to gain improper access to national security information;
>
> Those attempting penetration for "recreational" purposes (These are the "[computer] hackers" recently covered by the media.); and
>
> Those attempting to access Treasury voice (especially radio) communications to avoid detection or apprehension by Treasury Enforcement Bureaus.[16]

1. Privacy

Privacy in a technological age becomes a critical balance between effective use of technology and adequate protection of personal information. Chairman Glickman indicated that in many instances security breaches in computerized resources posed a threat to personal privacy. He urged the Office of Management and Budget (OMB), the central government manager to take an active role in improving Government computer resources security, not only to save money, but to prevent the erosion of the "privacy of millions of Americans." [17] The Chairman expressed concern that technological advances in information handling triggers this situation. He went on to say that:

> It seems to me that computer technology has carried us to communication and information advances that we never

[14] Ibid., p. 75.
[15] Ibid., p. 79.
[16] Ibid., p. 427.
[17] Ibid., p. 182.

> thought possible. But it looks to me like it's made stealing information a science and privacy an illusion.[18]

Dr. Ware indicated that many of the privacy questions and issues identified over the years had not been adequately addressed. Specifically, he commented that most of the recommendations that were made by the Privacy Protection Study Commission [PPSC] in the late '70s had not been implemented in law, and moreover some of the new dimensions of privacy had not been identified nor treated by the Commission. Dr. Ware's testimony highlighted some of these other privacy related problems:

> To date, privacy has been interpreted in the context of record-keeping processes, but it is clear that the widespread application of computer and communication systems to provide a broad spectrum of services will eventuate in many new dimensions of privacy.
>
> We are seeing the emergence of systems that contain vast amounts of information about people but not for record-keeping purposes. Let me illustrate in terms of electronic mail, which the U.S. Postal Service is promoting as E–COM. The purpose of such a service is to transport information from sender to addressee and to the extent that such information is personal in nature, the system will contain much information about people but not for record-keeping purposes. In addition to the message content, the system will contain information used to establish relationships among groups of people, such as organized groups or circles of acquaintance. Obviously, such information could be of high interest to the law enforcement community and others, but the legal umbrella of protection over it is confused and probably incomplete.[19]

Chairman Glickman, in raising the privacy issue asked the GAO the following:

> Do you see a danger that citizens will lose confidence in the government in its efforts to collect information on citizens as a result of concern over the security of computers and the information that is contained therein? [20]

Mr. Warren Reed, Director, Information Management and Technology Division, of the U.S. General Accounting Office (GAO) responded that this was a distinct danger, especially if the focus were not clear. Mr. Reed commented that although he did not believe that the alarm stage had been reached, he is concerned that "as time goes on, because of the threats and problems . . ." [21] that possibility exists.

[18] Ibid.
[19] Ibid., p. 463–464.
[20] Ibid., p. 220.
[21] Ibid.

2. Vulnerability and Threats

a. Personnel

Witnesses expressed concern that the greatest threat to computer systems continues to be people. Often the threat comes primarily from the authorized user or the staff person who has both the skill and authority needed to access the system. Dr. Willis Ware, in discussing threats from personnel, compared the differences in security management approaches between the Department of Defense and the commercial sector in dealing with the people problem:

> . . . let me contrast the security situation in the defense environment versus that in the commercial/industrial world.
>
> Within defense the threat against computer-based systems includes the full technical resources of advanced major world powers, where such threats can be mounted with substantial funding and other resources. In the Department of Defense context, therefore, the threat includes intense technical aspects as well as aspects involving people—such as buying them for subversive actions. On the other hand, the defense community does go through an investigative process to grant formal clearances to people; therefore, it has substantial assurance of trustworthiness.
>
> In the commercial sector, on the other hand, the technical threat is at present minimal. The big threat is people within the system themselves. If one examines, for example, the Parker/SRI data base of computer-related criminal actions, he finds that the great bulk of them have been perpetrated by an individual who was authorized to interact with the system and who knew enough about it to exploit it for personal gain. Furthermore, there is generally little attention paid in the commercial world to establishing trustworthiness of individuals in critical and sensitive positions within a computer-based information system. Some corporations do essentially nothing by way of assuring the trustworthiness of critical individuals; others take the minimal step of requiring that individuals are bondable—a real minimum level of assurance of trustworthiness; and very few, perhaps none, engage in a comprehensive background investigation.[22]

Dr. Ware went on to say that:

> When the private sector gets the "people problem" dimension of the threat against its computer system under control, and the simple technical threats protected against, then sophisticated technical threats will become more important.[23]

[22] Ibid., p. 456–457.
[23] Ibid., p. 457.

b. Computer Hackers

Extensive communication networks now link computers and associated information systems together. With this technological advance a new underground culture has emerged, personified in the term "computer hacker," and illustrated in the popular film "War Games". The short film clip from "War Games," shown at the hearing, illustrates the relative ease with which computers can be accessed by the unauthorized user.

Recently the activities of a group of computer hackers from Wisconsin, generally referred to as the "414's," received national attention. The "414's" over a period of time were able to access a number of Government and non-Government systems which used commercially available telecommunications network. Allegedly these computer hackers were able to access data systems at Los Alamos National Laboratories, Sloan-Kettering Hospital, and other locations.

While the computer hacker is sometimes viewed by others as harmless, his victims often do not share this view. Although the intent of these young hackers may not always be to harm the system or to obtain a monetary gain, computer hacking is a misuse of the system and represents a problem to users and the computer security manager. In his testimony Donn Parker detailed this phenomena:

> Computer hackers are hobbyists with intense interest in exploring the capabilities of computers and communications and causing these systems to perform to their limits. They are also called system hackers, or compulsive programmers, and often constitute subcultures within schools, computer clubs, and technological work environments. Hackers exhibit a spectrum of behavior from benign to malicious. Malicious hacking consists mostly of unauthorized access from a terminal connected by telephone to a dial-up-access computer owned by another party, followed in some cases by various acts of vandalism such as destroying or contaminating data, or use of computer services.
>
> Hackers generally attempt to rationalize their activities by indicating the great educational value and satisfaction of benign intellectual curiosity and experiment. Their definition of malicious hacking is quite different from that of the victims. Malice means to cause harm without legal justification or excuse or intent to commit an unlawful act. Malicious mischief is willful, wanton or reckless danger to, or destruction of, another's property. These latter definitions provide appropriate descriptions of malicious hacking from the victims perspective.[24]

Mr. Parker went on to say that there is a tendency for the media to misrepresent the nature of the computer hacker's actions. He commented that often the computer hacker tends to be viewed uncritically, if not admiringly, and that the media may even refer to them as "Robin Hoods of the Information Age."[25]

[24] Ibid., p. 74.
[25] Ibid., p. 75.

Furthermore, Mr. Parker said:

> The size of the problem is increasing as terminals, modems, and microcomputers become more available. Richard J. Matlack, President of Infocorp, a marketing research firm, estimates that there are about 600,000 computers used in homes, and 120,000 to 180,000 of them are equipment with modems used to gain access through telephones. Another contribution to the size [of the problem] is an increasing number of juveniles learning the technology; propagation of capabilities, and encouragement of young neophytes by older hackers is common. Many hackers claim they were taught and/or encouraged by older juveniles or adults. There is general advice, often heard, to engage in hacking before reaching the age of exposure to adult criminal prosecution. Particularly virulent pirate boards with new hacking intelligence also probably stimulate activity.[26]

Donn Parker summarized the types of losses that could be incurred by the actions of computer hackers:[27]

> Destroyed or contaminated data files and computer programs;
> Use of computer or telecommunication services or denial of use of such services;
> Theft of copies of programs or data for personal or associates use or gain; and
> Modification of program or data for personal or associate's gain.

The ranking Minority Member of the Subcommittee, Representative William Carney also expressed concern regarding the computer hacker problem:

> I believe that few of us realize the impact of computer technology in our daily lives. Every time we fill out a credit card application, apply for a bank transaction card or a loan, our names, addresses and financial data and employment status becomes part of a large information network that, without proper safeguards, can fall into the hands of computer hackers.[28]

The lead off witness at the hearings, a 17-year-old high school senior and a member of the "414's", Neal Patrick, admitted that he engaged in "systems hacking". He testified that his interest in computers began with an introductory course taken when he was in seventh grade. Eventually he learned various computer languages and by using his family's computer gained unauthorized access to certain systems. Mr. Patrick told the subcommittee that access to Government and private sector computers was often made possible by poor control of passwords. He described how members of the "414's" exchange information by using "electronic bulletin

[26] Ibid.
[27] Ibid.
[28] Ibid., p. 4.

boards". These boards enabled them to ferret out access codes and passwords which gain them access to targeted systems.[28]

In describing some of the events, Mr. Patrick disclosed that computer hackers had created a new account in the Los Alamos computer system so that they could continue to gain access. Ironically, they gave this new account or file the code name "Joshua," repeating the access code used in the film "War Games".

While the victim of the computer hacker seldom characterizes the trespass or tampering into his system as benign, the hackers may not recognize the wrong. Representative Bill Nelson questioned Neil Patrick on this matter. Mr. Nelson asked:

> Now, under previous questioning of the Committee, you have indicated that you saw after the fact that what you had done was wrong and that you had come forth and, thus, the cooperation with the authorities. At what point in this whole continuum of activity did you first question the ethical propriety of what you were doing? [29]

Mr. Patrick's reply: "Once the FBI knocked at my door." [30]

The perception that "no harm intended was no harm done" pervades the computer hacker mentality. While the computer hacker might never consider "breaking and entering" into anyone's home, he seems to lose those ethics when gaining unauthorized access to systems. This caused Representative Ron Wyden to speculate that there may be a need to include a section on ethics in basic computer courses.

c. Computer Crimes

Computer crimes are a relatively new aspect of white collar crime which have gained public attention. Mr. Parker defines computer crime as "any crime in which the criminal required specific knowledge of computers or data communication for its perpetration." [31] Mr. Parker commented that:

> There were no valid statistics on the size of the computer crime problem. We only know the nature of the problem based on a case-by-case, empirical analysis of known and reported cases that represent a limited collection of information. For example, most of the 1,100 cases in our research files at SRI were accidentally discovered and reported in spite of the reluctance of the victims to reveal their losses. Therefore, we wonder how many really smart perpetrators don't get caught, detected, or reported. I conjecture that there is an escalation of all kinds of business and white collar crime, not only computer crime, caused by the increasing use and dependence on computers and data communications. By the escalation I mean that frequency of crimes is diminishing while the size of each loss is increasing.[32]

[28] Ibid., p. 13–16.
[29] Ibid., p. 27.
[30] Ibid.
[31] Ibid., p. 72.
[32] Ibid.

To illustrate the scope of computer crimes Mr. Parker listed the following cases: [33]

1980: $1.2 million—The largest funds transfer fraud.
1980: 257 people killed—One of the severest airliner crashes caused by criminal negligence in programming a flight navigation computer.
1981: $21.3 million—The largest bank embezzlement.
1981: $53 million—The largest securities fraud.
1981: $50 million—The largest commodities fraud.
1982: $67 million—The largest inventory fraud.

Mr. Parker explained that:

> These massive crimes were all facilitated by two facts: (1) A concentration of information assets was being stored, processed, communicated and output by computers and telecommunications systems, and (2) these assets were removed from direct human view or evaluation and safeguarding.[34]

Lloyd Clark, Assistant Director the Federal Bureau of Investigation gave another perspective on computer crime. He stated that: [35]

> I would like to point out three things that we in the FBI believe are key to understanding the FBI's perspective on computer-related crimes.
>
> The first of these issues is that a computer is an instrumentality of some other form of traditional crime, for instance, theft or larceny. It is much like a gun, a knife, or a forger's pen.
>
> The second issue is of a more academic nature, but nevertheless important in that there does not exist, at this time, one generally recognized and accepted definition as to what computer crime is. Therefore, we do not have an objective standard to measure the trends of computer-related crime.
>
> Last, in the view of the FBI's current structure of management by program, rather than by case, there is no method in place now to observe the statistical dimensions of computer-related crime.

d. Poor Password Management

Passwords are analagous to safe combinations in that they provide a control or special instruction to the computer to permit access to the information it contains. In the film "War Games" the young computer hacker is shown gaining access to the school computer via a purloined password. Neil Patrick testified that it was not always necessary to steal a password as some passwords are set up by the makers of the computer or software system. He observed that these vendor-given passwords are well known and appear in the vendor's manuals. Therefore a large number of computers

[33] Ibid.
[34] Ibid.
[35] Ibid., p. 44.

around the country have the same passwords.[36] This condition results from the fact that often the system operator has not taken the time to change the passwords. Therefore, failure of systems planners to change the vendor-given password facilitates unauthorized users accessing a system. Mr. Patrick told the Subcommittee that the computer hacker would be confronted with a great many difficulties if vendor-given passwords are changed. In fact he acknowledged that it would have been virtually impossible to access a system without knowledge of the password. Moreover, he said that an unknown long password, because of the sheer number of characters that could be chosen, might require a computer over ten years to discover.[37]

The intrusion into the Los Alamos National Laboratories computers was made possible because systems passwords had not been changed when the system was installed. The password used by the perpetrators in that instance came from the Digital Equipment Corporation [DEC] manual. In discussing this poor control of passwords, Mr. McClary, Division Leader for Operational Security and Safeguard Division at Los Alamos, described it as "disappointing" that the password was not changed when the system was installed.[38]

e. Implications of Technological Innovation

When a new technology is implemented, traditional protections may not always be sufficient to safeguard the process. Dr. Ware gave the example of electronic mail systems, where a range of security and privacy problems unknown in the traditional mail process may emerge. For example, the files created by the electronic mail system are likely to become a "comprehensive business record" system and accessing such information systems may present a special set of problems. Dr. Ware in discussing these problems posed the following questions:[39]

> Who owns information in an electronic mail system?
> Does the owner of the computer system own it?
> Does he have a right to witch hunt through that information as he sees fit?
> What is the situation for intrastate offering versus interstate offering and in the long-run international offerings? What is the search and seizure situation? Can the private vendor be given legal standing to resist?
> What is his obligation to his users in case of an attempted seizure?
> What is his liability in case the system misbehaves and loses mail records?
> What is his responsibility in case the system improperly spills information to a wrong party?
> What is his responsibility if maintenance people see that information and use it for private gain, political advantage, private harassment, or whatever?

[36] Ibid., p. 17-18.
[37] Ibid.
[38] Ibid., p. 42.
[39] Ibid., p. 452.

What are the vendor's obligation to provide comprehensive safeguards? Should they be mandated by law?

3. Countermeasures

Safeguarding computer/communications systems requires taking the appropriate measures. The protective measures range from improving control (physical access, password, etc.) to implementing sophisticated technological innovocations.

a. Better Management Controls

Many of the witnesses urged that management should improve access controls, such as passwords. Mr. Neil Patrick described what is initially needed to safeguard systems.[40] He pointed out that:

> There is no need for million-dollar security measures, but just commonsense ideas and attitudes would prevent most of this, if not all of this from happening.

Another means of control was discussed by Willis Ware. He commented that:[41]

> When an individual logs on to a computer system, he is normally requested to supply personal identification and a password which, in effect, is an authentication of his identity. Someone attempting to penetrate a computer system tries to guess his way in by masquerading as a legitimate user. Most systems today permit an indefinite number of log-on trials. It therefore is feasible for a perpetrator to program a small computer systematically to try words, combinations of letters and characters, or other possible passwords until one is found that works. Clearly, this is an undesirable and unsafe arrangement. There is no reason why a computer should not disconnect an individual after some number of attempts, such as three or five, and keep him disconnected until his authenticity has been assured.

Dr. Ware referred to another method to combat unauthorized users access. He noted that:

> Since every computer system has to be started at some time, invariably there is a mechanism for accomplishing what is called the initial software load. Often this takes the form of a button, a switch, or a sequence of actions by the console operator. Imagine a scenario in which an operator on the graveyard shift finds the machine inactive and decides to do something in his own behalf such as illegally copying a sensitive file of information. Having done so, he simply reloads the machine as though it had stopped for some reason; there will be no record of what he has surreptitiously done. There are obvious technical offsets to such malfeasance by operators, but they do not exist in marketed machines. Even the procedure of two-person control used by the military would be a deterrent.[42]

[40] Ibid., p. 19.
[41] Ibid., p. 459.
[42] Ibid., p. 460.

Selecting the appropriate computer security measures should be considered in the initial design phase of any project. Retrofiting security safeguards are quite difficult and may not be as effective. In summarizing this Dr. Elmer Clegg of the Honeywell Corporation urged that in:

> . . . recognition and definition of computer requirements in the design phase of a system is critical, especially in the areas of communications security and operating systems security. Security of these types are difficult to achieve as an "add-on" to an existing system. The initial design must contain certain characteristics to provide this capability and therefore must become more important in the procurement process.[43]

b. Raising Public Awareness

Representative William Carney, Ranking Minority Member, suggested that perhaps on a practical level increasing public awareness is an approach which might help in protecting computerized resources. He commented that:

> One of the points I was trying to make, and I think my colleague, Mr. Wyden, in his conclusion made that same point, is that perhaps we all recognize the importance of making the public aware of the fact that computers can be very easily accessed. But I think what we're trying to establish is how to prevent that. And it seems to me . . . that perhaps it's not so much government's role to come out, spend an enormous amount of money trying to prevent this type of thing, or to promulgate an enormous amount of rules and regulations in public law, but a little common sense by the user can very well be the best way to prevent this type of access.[44]

Representative Carney commented that at these hearings we have done a public service by alerting everybody to the ease of access which is possible when these everyday home computers and computers that use telecommunications lines are used. He went on to say that raising public awareness "might be the greatest role we, as a government can do."[45]

c. Technological Protective Measures

Computers and communications systems can be protected in many ways. Witnesses at the hearings alluded to a wide range of innovations from passwords to advances in operating systems security. The prime focus in the Department of Defense for developing technological security measures is the DOD Computer Security Center. The Center sponsors research in "trusted" computer technology. Its recently completed "DOD Trusted Computer System Evaluation Criteria" is directed at providing: [46]

[43] Ibid., p. 527.
[44] Ibid., p. 32.
[45] Ibid., p. 33.
[46] Ibid., p. 277.

> Users with a metric with which to evaluate the degree of trust that can be placed in computer systems for the secure processing of classified and other sensitive information;
>
> Guidance to manufacturers as to what security features to build into their new and planned, commercial products in order to provide widely available systems that satisfy trust requirements for sensitive applications; and
>
> A basis for specifying security requirements in acquisition specifications.

The "evaluation criteria" are being used by computer manufacturers, and are beginning to influence security products. Mr. Clegg testified that progress continues to be made in hardware and software innovations having strong security features tied to the guidance given by the Center's "evaluation criteria".

As has been mentioned, computers and other electronic information processing equipment emit signals which can be intercepted and interpreted by certain devices. Representatives Albert Gore questioned Mr. Mclary of Los Almos National Laboratories regarding the possibility of interception of information due to emanating signals (electronic radiation). Representative Gore commented that: [47]

> You've got a computer at Los Alamos and somebody has a car in the parking lot with a receiver that's capable of picking up the radio interference and, from those radio waves, reconstructing the movement of the central processor unit and printing out what it is that's occurring on your computer.

Representative Gore went on to say:

> . . . with the proper equipment, one can listen to waves emanating from an electric typewriter and reconstruct everything that a typewriter is typing.

Mr. McClary responded that steps are taken by Federal agencies to prevent compromising emanations. The Federal Government requires the use of TEMPEST—approved word processors and computers for handling national security classified information. The Department of Defense government-wide TEMPEST program is designed to limit emanation problems by protecting electronic equipment (such as network technologies) which handle classified data.[48]

d. Legal Countermeasures

Changes in the law were viewed by some witnesses as a viable means to counter abuses. Specifically, they expressed the opinion that a law to protect against intrusions or penetrations into computer systems would be useful. Some types of computer abuses may be prosecuted under existing statutes for stolen property, privacy violations, etc. (See Appendix B for a list of statutes which can be used in cases of computer abuse). But, present legal remedies are

[47] Ibid., p. 47.
[48] Ibid.

not always sufficient to cope with some innovative computer/communications systems penetrations. Several witnesses supported expansion of statutory language to include certain types of computer abuses such as trespassing or browsing. For example, Mr. McClary suggested that there was a need for a legal deterrent to make people accountable for any damages and costs that might be incurred from unauthorized access. He expressed support for legal remedies which would provide the same protection for information systems as for material property.[49]

Donn Parker also recommended that "explicit Federal and State criminal statutes should be enacted to allow a vehicle for vigorous prosecution." [50] These explicit laws, Mr. Parker believed, would serve to deter some systems abuses.[51]

The General Accounting Office expressed concern about the lack of appropriate remedies for computer abuses. They indicated support for improving existing laws, such as the Omnibus Crime and Safe Streets Act, Section on Wiretapping and the Communications Act of 1934. Like other witnesses GAO concluded that there is a need to clarify which types of data interception are illegal.[52]

C. LEGAL ASPECTS AND LEGISLATIVE DIRECTION

Existing laws such as the Privacy Act of 1974, the Financial Management Integrity Act, the Foreign Corrupt Practices Act, and those discussed in section C of chapter I provide a framework for computer security management in the private and public sectors. Other laws protecting government property and resources, trade secrets, wiretapping, and data confidentiality have been used to protect against computer abuse.

1. Computer Crime Legislation

While the hearings did not focus on the legislation pending in the 98th Congress, witnesses made direct and indirect references to some of the measures. Bills concerning computer security and computer abuses pending in the 98th Congress include the following:

H.R. 1092 (Nelson)/S. 1733 (Trible). *Federal Computer Security Protection Act.* Amends the Federal criminal code to establish penalties for using or attempting to use Federal computers, certain financial institutions, and those that use interstate facilities with intent to defraud, obtain property by false pretenses, embezzle, steal or knowingly convert the property of another.

H.R. 3075 (Wyden)/S. 1920 (Tsongas). *Small Business Computer Crime Prevention Act.* Amends the Small Business Act to establish a Small Business Computer Crime and Security Task Force and an information clearinghouse to assist the small business community.

H.R. 3570 (Hughes). Amends Title 18 U.S.C. to provide penalties for counterfeiting of access devices (credit cards).

[49] Ibid., p. 51.
[50] Ibid., p. 71–73.
[51] Ibid., p. 72.
[52] Ibid., p. 198.

H.R. 4301 (Coughlin). Amends Title 18 U.S.C. to provide penalties for certain computer-related crime.

H.R. 4384 (Mica). Establishes the Computer Security Research Program and the Interagency Committee on Computer Crime and Abuse, and provides penalties for computer abuse.

H.R. 4954 (Wyden). A bill to penalize unauthorized direct access to individual medical records through a telecommunications device.

S. 1733 (Trible). A bill to amend title 18, United States Code, to make a crime the use, for fraudulent or other illegal purposes, of any computer owned or operated by the United States, certain financial institutions, and entities affecting interstate commerce.

S. 1920 (Tsongas). A bill to amend the Small Business Act to establish a Small Business Computer Crime and Security Task Force, and for other purposes.

S. 2270 (Cohen). A bill to amend title 18 of the United States Code to prohibit the use, for fraudulent or other illegal purposes, of any computer owned or operated by the United States, certain financial institutions, and entities affecting interstate commerce.

Some of this proposed legislation would make computer abuses and misuses a Federal crime. Some witnesses thought passage of some of these measures would help. Specifically they claimed that:

> Prosecution would be facilitated; public awareness would be increased; and better laws would serve as a deterrent.

The General Accounting Office commented that without a specific statute it is clear that an effort to modify or steal data or resources might be covered by existing laws but, there may be a "hybrid area where you may or may not have a Federal crime." [53]

a. Call for Clearer Definitions

Joseph Wright of the Office of Management and Budget (OMB) suggested that a clearer definition of computer crime in Federal legislation might provide a framework for prosecuting offenders.[54]

The GAO commented that clarity of definitions also was needed in existing statutes. Specifically they commented that:

> [A] review of applicable telecommunications security legislation showed that the Communications Act of 1934 and the Crime Control Act of 1968 are inadequate with respect to interceptions of wire communications, or "wiretapping." The 1934 Communications Act did not define the term "interception." The Crime Control Act of 1968, as amended, used the qualifying term "aural acquisition" (acquired by use of the ear) to define interception. As a result, only interceptions by aural means are illegal under this act, unless authorized by court order. Therefore, we conclude that as long as the term "aural" remains as a semantic qualifier in the 1968 Crime Control Act's definition of interception anyone can conduct unauthorized nonaural wiretapping of data telecommunications without a court order and not be in violation of this law.[55]

[53] Ibid.
[54] Ibid., p. 118.

Concern for unauthorized access to computer systems as demonstrated by the involvement of the hackers in Milwaukee led Chairman Glickman to ask the FBI if the "mere unauthorized access, the intentional unauthorized access into somebody else's computer, is a crime under current law?" Floyd Clarke, Assistant Director of the FBI Criminal Investigative Division, replied:

> Not necessarily. It is possible for an individual to gain access into a computer into the system, and if there is no damage nor information acquired, that in and of itself would not constitute a Federal crime.[56]

The Chairman questioned further "if there is no damage, but the invaded systems has caused some degree of delays or costs in terms of getting their system back to where it was before, would that constitute damage?" Mr. Clarke responded that:

> . . . I think that's part of the problem that we need to look at in any legislation that may be addressed, the definition of the term damage. And also—dealing with the concept of trespassing into a computer.[57]

b. Intrusion and Unintentional Trespass

Witnesses agreed that the legal status of computer intrusions is difficult to assess without concise definitions. Robert Morris, a computer security expert with the Bell Telephone Laboratories, called attention to the lack of a precise understanding of the legal status of computer intrusion. He indicated that:

> It is not all clear at this point whether mere intrusion into a computer system, whether in an intrastate or interstate situation, is or is not a criminal activity.[58]

He went on to say that he would welcome "a clearer definition, such as we have for the interception of communications, where the statutory situation, although quite mixed, is perfectly clear" to those with a civil or criminal responsibility." [59]

Mr. McClary of Los Alamos National Laboratory also alluded to the legal problem of the unauthorized intruder's "intent" as a significant element. He commented that intent enters into much of our legal system and it may be appropriate in this context. He reflected that with regard to property, "unintentional trespass occurs, and our legal system handles it quite well." Mr. McClary suggested that the same legal protection given to materials or property might be extended to the protection of information resources and capabilities. And that this ultimately should be the goal of legislation designed to protect these resources.[60]

[55] Ibid., p. 198–199.
[56] Ibid., p. 418.
[57] Ibid.
[58] Ibid., p. 510.
[59] Ibid.
[60] Ibid., p. 51.

2. Responsibility, Ownership, and Liability

a. Electronic Mail Systems

As mentioned above the apparent lack of legal protection in determining responsibilities and liabilities for misuse or abuse of information in certain systems prompted Dr. Willis Ware to raise another problem. He referred to a specific incident in which the electronic mail system in a Government agency had been accessed for internal investigative purposes. He claimed that the case involved a Federal agency in which internal investigators had arranged for a complete computer printout of employees' electronic mail records. In such a situation it is not clear if privacy rights in an electronic system have the same protections as those of the traditional manual mail handling system.[61]

b. Vendors Responsibilities

The issue of vendors' obligations to provide comprehensive safeguards was raised. Dr. Ware questioned whether vendors should be mandated by law to provide certain safeguards.[62] It is unclear what the vendors' responsibility is regarding product performance guarantees. Proper software performance is difficult to ascertain because of the different approaches a program may contain.

Mr. Jack Hancock, Senior Vice President for Corporate Strategy and Systems of Wells Fargo Bank, pointed out that there may be a need for a "certification procedures to validate equipment, techniques, and software. This process would assure the buyer that the products met the specifications that the vendor claims." [63]

D. LEADERSHIP ISSUES

Leadership values concern both the national interest and Federal Government programs effectiveness. While the Subcommittee's hearings focused attention on the development of a strong leadership for computer/communications security there was considerable variation as to the approaches which should be taken. This section discusses the need for national direction, a strengthening of Federal computer security programs, the role of Federal central management agencies, balancing national security and civilian requirements, research and development, and private sector initiatives.

1. Lack of Strong National Leadership

The lack of a clear and well defined set of national goals protecting computer and communications systems continues to be a serious limitation in establishing an effective national program.

The lack of clarity in the Federal position is illustrated by Federal policies designating communication security responsibilities. An unclassified abstract of Presidential Directive 24 (PD–24), which outlines Federal communications security policy was criticized by the GAO for failing to clearly state the distinct responsibilities of the National Security Agency and the Department of Commerce. The General Accounting Office testified that in its review of Federal data network security management it examined PD–24 and found it to be less than adequate in pinpointing responsibility. The GAO reported at the hearings that the Administration had informed them that this Directive was under review by the National Security Council (NSC) for possible changes.[64] More recently the Congressional Research Service also inquired of the NSC if PD–24 had been revised and learned the revision is still pending.

[61] Ibid., p. 449.
[62] Ibid., p. 452.
[63] Ibid., p. 487.

Other aspects of the Federal computer security management effort also lack clarity. A well defined set of computer security directions for Federal agencies is generally lacking. Willis Ware alluded to this problem and suggested the need for a more cohesive approach. He stated that:

> . . . what the government needs is a comprehensive, let us call it a, handbook that says here is how one runs the computer center security program; here are the procedural and administrative safeguards that must be in place; here are the risks that people represent; here is what can be done against those risks; and here are the administrative protective measures that can be taken. . . .[65]

Dr. Ware went on to say that:

> No entity in government has addressed the general policy issue of what constitutes a compehensive top-to-bottom prescription for installing security controls, nor identified the many dimensions of such policy and made it available as guidance. It is being done piecemeal; every agency is inventing it for itself or not doing it.[66]

The lack of a strong central Federal focus for computer/communications security and unclear government policies, according to some witnesses, is to blame for poor computer/communications security planning. In some instances it was not clear what direction is provided to agencies nor what encouragement is given to improve Federal computer/communications security planning.

2. Federal Leadership and Initiatives

Requirements for protecting computer/communications systems vary considerably among Federal agencies. The distinction is especially acute between those agencies handling national security classified data and those who do not.

For those in the national security community and other agencies handling classified data, guidance is derived from certain presidential directives. Therefore these Federal Agencies, along with their contractors must conform to requirements for handling classified data and use prescribed security measures to prevent unwanted disclosure. On the other hand, there is no such guidance for non-national security information. (See section E2 for additional discussion of this issue.)

[64] Ibid., p. 223.
[65] Ibid., p. 462.
[66] Ibid.

a. The Role of the Office of Management and Budget (OMB)

OMB is the lead central management agency and is responsible for establishing Government-wide computer/communications policy for the non-defense agencies. The General Services Administration, Office of Personnel Management, and the National Bureau of Standards also provide guidance to Federal agencies regarding planning and managing of computers and associated resources. The mission agencies are responsible for assigning the level of data protection except for those agencies handling classified data. Overall security policy in non-national security data systems is articulated in OMB Circular A–71, Transmittal Memorandum No. 1 (sometimes referred to as TM–1). TM–1 provides general security guidance. With regard to privacy protections OMB Circular A–108 provides guidance for the "systems of records" defined by the Privacy Act of 1974.

OMB testified before the Subcommittee that it was planning to review and consolidate its guidance concerning Federal information and automatic data processing. While this represents a positive step OMB did not indicate it had any special plans to monitor agency implementation of computer security programs. Nor did OMB indicate any explicit reviews of agencies' risk assessment plans or special coordination of any other computer security initiatives at this time.

OMB also discussed its role in providing Federal agencies computer security management guidance, and referred to the issuance of TM–1 requiring agencies to submit computer security plans for review. Although this initial stage was completed by OMB, no further review is being contemplated.

Joseph Wright, OMB Deputy Director, admitted in testimony before the subcommittee that it:

> required agencies to submit their plans for implementing the memorandum for OMB review, and a full review was done at that time. It has been updated through a series of processes, but we have not repeated that exercise because we felt at that stage we were able to go on ahead and focused enough attention from the agencies as to the needs for computer security.[67]

OMB testified that on September 12, 1983 it had given notice in the *Federal Register* of consolidation of some of the existing OMB circulars pertaining to computer/communication systems.[68] Mr. Wright stated that:

> Things are changing dramatically . . . The rapid growth and the reliance on information technology really brings to the front the need for an effective Federal computer security program. We don't have enough coverage in areas like microcomputers. We also don't have enough coverage in terms of the areas of telecommunications. These areas were not a major focus during the mid-1970s.[69]

[67] Ibid., p. 103.
[68] Ibid., p. 185.
[69] Ibid., p. 103.

Wright also indicated that the Administration was examining the problems of computer fraud and abuse in Federal programs. He pointed out that a recent report by the President's Council on Integrity and Efficiency on Federal computer fraud and abuse indicated a low number of incidences of computer crime. He went on to speculate that this may indicate two things: "Either it is less of a problem than we thought—but my guess is that the reporting vehicles that we have are probably not appropriate, and we simply were not able to identify many of the cases." [70]

Other OMB policies and programs which have implications for safeguarding information include the following:

Information Resources Management Reviews—required under the Paperwork Act of 1980;

Review of computer matching operations; and

Budget review process which will also consist of a full management review of agency programs including ADP security plans.

b. Criticisms of the OMB Approach

OMB has been specifically criticized for not providing effective leadership for Federal computer/communications security programs. For example, when questioned on the adequacy of manpower to give guidance to Federal agencies, Mr. Wright stated that there was a need to upgrade OMB's security resources. Furthermore, in response to a question regarding the number of OMB personnel available to guide agencies on security matters, Mr. Wright was unable to identify the specific number of dedicated computer security specialists at OMB. OMB admitted that it resorted to detailing technical experts from other agencies, such as the General Services Administration and the National Bureau of Standards, to meet its needs in this area.[71]

GAO expressed concern that there was a need for a comprehensive policy and that OMB was overdue in examining this issue. GAO indicated that although the OMB was in the process of updating some of the relevant OMB circulars there was no indication that they would incorporate any provisions of the internal controls dictated by OMB Circular A–123, "Internal Control Systems," into this planned revision. GAO suggested that other policies could be merged. Specifically Mr. Reed urged that:

> . . . internal control policy [OMB Circular A–123] and computer security policy as represented in Transmittal Memorandum No. 1, both serve to safeguard agency assets from waste, loss and abuse and should be considered essential tools for information resources management and should be considered together.[72]

GAO expressed reservations that OMB might believe that by issuing policies it had resolved all the problems. They argued that OMB could improve agency compliance with policy initiatives if it provided systematic reviews. Furthermore, GAO urged that OMB

[70] Ibid., p. 103.
[71] Ibid., p. 104.
[72] Ibid., p. 270.

should encourage Federal agencies to follow through on plans for information security and plans to test and evaluate the results of the safeguards.

3. Balancing National Security and Civilian Needs

Another important problem confronting computer security is meeting the legitimate goals of the national defense community and, at the same time, the requirements of the private sector. While the stringent national security and intelligence computer/communications security requirements are understood, there is concern about allowing the national security community broader controls over developments in this area. With the increased private sector interest in computer/communications security there is need to share both security responsibilities and resources.

One witness, Steve Walker, President of Trusted Information Systems Inc., acknowledged that this balance was made difficult because of the diversity of requirements between the private and defense sectors. He cautioned that while the DOD has "reasonable capability" as a result of the newly established Computer Security Center [sometimes referred to as the Computer Security Evaluation Center (CSEC)], that organization should not necessarily be viewed as providing advice to all parts of the government. He warned that:

> The DOD CSEC cannot and must not assume the role of giving advice to the other Departments of the Federal Government. Situated as it is in the Intelligence Community such a role would be, I believe, most inappropriate.[73]

He went on to say that:

> Prior to founding the Center at NSA, consideration was given to forming a Federal Computer Evaluation Center, located at NBS and jointly administered by DOD and the Department of Commerce. However, considerable resistance to such a facility arose within DOD and there was little support for the idea from other elements of the government. It was recognized at the time of the decision to locate the DOD center at NSA that this would have a limiting effect on the applicability of its results to the rest of government.[74]

Futhermore, Walker advised that:

> Some means must be found for offering direct support to the major elements of the Federal government because the computer security aspects of the Social Security, IRS and similar activities are very serious. Establishment of a Federal Center, working closely with the DOD Center is a possibility and NBS remains one of the few logical choices for such a facility. But it will be essential (and very difficult) to ensure that the two organizations do not overlap, or worse, contradict each other.[75]

[73] Ibid., p. 95.
[74] Ibid.
[75] Ibid.

Regarding the Federal government's role for the private sector Walker suggested that:

> Government should limit its efforts to a major education and awareness program concerning vulnerabilities and available solutions. Such an effort coupled with the evolution of market forces should be sufficient to advance the state of the art for at least the next few years.[76]

Another area which has demanded a balanced approach is data encryption. Cryptology, once a government monopoly, is now of increased interest to the private sector. The National Bureau of Standards, stimulated by the Privacy Act of 1974, issued the Data Encryption Standard (DES), a government approved cryptological standard, which is an algorithm for encoding non-national security classified data. This action has contributed to the development of a new computer/communications security marketplace. New computer security tools which use the DES are being used in securing telecommunication supported automated information systems.

The Director of the DOD Computer Security Center, Mr. Melville Klein reported that:

> Domestic manufacturers may now submit DES-based equipments to NSA for evaluation against this standard [Federal Standard 1027]. NSA will formally endorse those equipments that meet FS1027. This program is operating very successfully with over 20 manufacturers of DES products participating. A direct result of this process is a rapidly growing set of endorsed commercially available equipments available to the U.S. to meet both national security related and private sector telecommunications protection needs.[77]

Another area that has required delicate balancing is the voluntary review of private sector cryptological research. (See discussion below.)

4. Research and Development

The hearings identified some major areas in which computer/communications security technology may need improvement. Development of effective tools and techniques was deemed essential to improving security of automated information systems. Specifically, the need to enhance performance and bring down cost of security technology is considered essential.

Mr. Walker expressed concern that there has not been a sustained effort to develop computer security technology. He commented that:

> There is a growing tendency to use add-on security packages to attempt to enhance the integrity of existing systems. If these systems, with their limitations, are fully understood and carefully employed, they can contribute a degree of protection that is not available in present day commercial systems. Unfortunately as the extensive histo-

[76] Ibid.
[77] Ibid., p. 401.

ry of systems penetration efforts over the past decade has shown, if these add-ons are blindly applied and relied on for full protection, they can be easily circumvented.[78]

In Mr. Walker's view there is a need to expand the scope of present computer security research. Mr. Walker summarized this perspective:

> Following my four years of sponsoring research in trusted computer systems at DARPA [Defense Advanced Research Projects Agency], I was convinced that in order to make real progress, the computer manufacturers must get deeply involved. The steps needed to build a trusted system start with the very innermost functions of a computer operating system and its hardware support. Unless and until the computer manufacturers understand and begin to utilize and improve upon the technical solutions presently known, further government research would only produce additional testbed demonstration systems. Government funded research pointed out several viable approaches to building trusted systems; now we need to leverage that research by reaching out to the development and engineering centers of the manufacturers to get them involved. This was the major focus of the DOD Computer Security Initiative from 1978 until 1981 and it has had considerable success. Several manufacturers now have significant efforts aimed at building high integrity trusted systems and more are getting involved daily. These systems are not easy to build, requiring several years to evolve into useful systems; but once available they promise to provide facilities that are resistant to hackers, malicious or not.[79]

a. DOD Computer Security Center Effort

The DOD Computer Security Center, administered and managed by the National Security Agency (NSA), is responsible for encouraging research to improve computer security. The Center was established in mid-1981 and the implementing directive (DOD Directive 5215.1) was issued in October 1982. The Director of the Center, Mr. Klein, described the Center's five pronged mission as including:

> First, to develop and promulgate uniform computer security criteria and standards that will lead to widespread availability of "trusted" products from computer vendors (Computer Security Evaluation Criteria). Second, to evaluate vendor products against these criteria and Third, to assist defense acquisition authorities in specifying and certifying trusted products in defense systems. Fourth, in research to improve the state-of-the-art in trusted computer technology and verification tools and methodologies. And, lastly to strengthen the computer security awareness and competence in the national security establishment through

[78] Ibid., p. 93.
[79] Ibid., p. 93.

> specialized training, seminars, information dissemination and ready access to evaluation resources.[80]

Research in computer security areas tends to be sensitive and therefore, there is a desire to control many research aspects. While the Center's activities are directed at promoting private sector development of certain protective measures, NSA has also been aware of the fact that disclosure of certain research would be harmful to foreign intelligence collection and the NSA communication security activities. Therefore, NSA has supported the development of a voluntary review of private sector cryptographic research papers. Klein's testimony provided the background to this voluntary review program. He reported that:

> In 1979 Admiral Bobby Inman [then director of NSA) spoke out publicly about articles and monographs written on cryptography. While he recognized the growing need for cryptography in the public sector, he believed that uncontrolled publication of cryptographic papers could be harmful to the foreign intelligence and COMSEC (NSA Communication Security) missions of the NSA. In response to this concern, the American Council of Education, through a National Science Foundation grant, sponsored a study group to review the issues. That Group, the Public Cryptography Study Group, was composed of members of various professional organizations and technical societies (e.g., IEEE and the Association for Computing Machinery) and the NSA's General Counsel. In 1981 the Group issued a report calling for a system for voluntary pre-publication review.[81]

Mr. Klein pointed out that NSA had reviewed over 100 papers and only a handful of issues have arisen. In three cases, he reported, NSA asked that the papers not be published. In Mr. Klein's opinion, the "chilling effect" that critics of this review procedure had predicted had not materialized.[82]

b. National Bureau of Standards Activities

The National Bureau of Standards (NBS) Institute for Computer Science and Technology (ICST) has a leading role in the development of computer security technology. In testimony John Lyons, Acting Director, National Bureau of Standards, identified the major computer/communications security thrust of ICST. In addition, he indicated that security technology might be integrated into existing and newly emerging application areas such as: [83]

> Network integrity and security in the ISO layered communications architecture;
> Cryptographic key management in computer telecommunications networks;
> Improved methods of personal identification for controlling access to computer networks;

[80] Ibid., p. 399.
[81] Ibid., p. 401.
[82] Ibid., p. 402.
[83] Ibid., p. 262.

Integrity/security architectures of personal computers;
Integrity/security protocols of transactions initiated from home telephones or home computers;
Methods for generating digital "signatures" on electronic messages, contracts, etc.
Methods for providing security to voice initiated computer transactions and to computer generated voice responses; and
Assessment of traffic flow security/privacy procedures on computer telecommunications networks.

Dr. Lyons suggested that this research might be useful in new applications such as "home banking, home voting/polling, electronic mail (voice and data), home initiated purchasing transactions, electronic contract negotiation, digital signature notarization of contracts, remote office operation, and computer software copyright protection." [84] He concluded that:

> Research in the above areas will involve several technical disciplines. Personal identification technology must be investigated to determine what characteristics can be easily determined to distinguish one person from another. Computer, electronic and telephone technologies must be used in developing cost-effective methods of implementing the needed security provisions. Many of the specialty fields of mathematics must be used to develop and evaluate cryptographic methods for assuring adequate integrity and security. Inexpensive methods for assuring physical and electronic security for the devices implementing computer and telecommunications security must be investigated.[85]

c. Other Research Approaches

Another view of national research directions was provided by Mr. Jack Hancock of Wells Fargo Bank who urged that a research and development group be created "to look at . . . very real but mundane and pedestrian issues dealing with security." He went on to suggest that consideration be given to a certification process and a national institute to provide a focus. He elaborated on these two concepts: [86]

> . . . there are many initiatives in computer security devices and techniques. Every week seems to bring a new one to the market. However it is virtually impossible for a single private organization or even a grouping of organizations to research these, assess their effectiveness, and integrate their implementation effectively.
> Therefore in this connection, there is a need for assistance to the private sector at two levels:
>
> > A certification procedure by an independent agency certifying that a device or technique meets specific minimum requirements. Private sector companies should be free to acquire or implement such devices

[84] Ibid., p. 263-264.
[85] Ibid.
[86] Ibid., p. 487.

> and techniques as they desire, but the certifying process would give them confidence that they are getting the capability specified by the vendor. This is a very complex area and should be carefully studied, however, it would seem to have merit.

Mr. Robert Campbell, a well-known computer security consultant, has suggested that there is a need for an *independent, privately-supported facility* to provide computer security research for the private sector. We support the creation of such an institution, but believe that its success will depend on full support of the Congress and the Executive department.

d. Private Sector Research Initiatives

Progress is being made on research and development of computer-communications security devices and products. The Government/industry partnership being fostered by the DOD computer security center program is expected to stimulate security innovations. Mr. Elmer I. Clegg of Honeywell Information Systems, Inc. indicated that while Honeywell had provided support to many areas of computer security, progress is being made, particularly in the area of operating system security. As an extension of MULTICS (a set of hardware and software measures with strong security features), the Secure Communications Processor (SCOMP) system has been introduced. Mr. Clegg stated that the SCOMP, has facilitated security and "bridges the gap between computer security research and available standard products." [87]

E. OTHER INITIATIVES AND APPROACHES

Witnesses suggested a wide range of remedies, some which are directed at coping with certain immediate problems and others that examine the problem from a national perspective.

1. Establishment of a National Commission

Willis Ware and others suggested the establishment of a "congressionally chartered commission" which might address broad issues related to security, especially those that transcend special interests or jurisdictional boundaries. Such a commission could examine the problems relating to the security of computer/communications systems.

In suggesting the establishment of a Federal or national commission to examine the problems, Ware suggested that the tasking effort should include the problems of information handling such as:[88]

> Computer-related crime; new dimensions of privacy; national vulnerabilities; new representations of information; problems of assessing and protecting intellectual property; problems of personal identification of individuals; and dislocations of power in this information revolution.

[87] Ibid., p. 526.
[88] Ibid., p. 469.

Donn Parker of SRI International also recommended that consideration be given to establishing a national commission. He felt that this commission should be broadly constituted. He alluded to a "national commission on information crime" which would "focus on the assets subject to loss rather than the instruments of causing that loss." [89] He went on to say that he favord a focus on "information crime rather than on computer crime, because computer technology changes so rapidly, and I would hate to see this . . . become outmoded very quickly." [90] He went on to note that information crime is a new concept and, ideally speaking it seems straightforward and simple, but practically, it may be quite complex." [91] Mr. Parker went on to say:

> I support Mr. Wyden's bill, H.R. 3075, and suggest that my recommendation is really an expansion of what he has proposed in his bill by having a national commission covering the whole subject of information crime and security rather than just for small business.
>
> I also think in Mr. Wyden's bill, there is a very important concept, and that is of having a resource center available to business organizations to help them with their problems having to do with information crime, and also having to do with security advice. I would think that a department in which this might be focused would be the Department of Commerce, and that would give this the breadth of advice that would be most practical in this regard.[92]

Hancock also cautioned that a national commission not be construed too narrowly. He expressed concern that:

> . . . if a commission is created and approaches the problem from the national security standpoint alone and deals with very high-level issues of defense, the National Security Agency and defense-related industry it will be, in the long term, less effective than if it is able to deal with the pure commercial private sector problems and the public awareness areas, about which nothing has been done in the past.[93]

2. Non-National Security Classification Schemes

Federal agencies handling national security classified information utilize a hierarchical scheme which includes designation such as confidential, secret, top secret, and various code word compartments. These designations influence the application of computer security safeguards. Consequently, automated information systems in these agencies use this scheme to apply the appropriate security measures. On the other hand other Federal agencies who do not handle classified data do not have a similar guiding mechanism. Chairman Glickman questioned—if a "system for classifying non-national security data according to the need for protecting it had

[89] Ibid., p. 71.
[90] Ibid.
[91] Ibid.
[92] Ibid.
[93] Ibid., p. 489–490.

ever been considered." Mr. Wright responded that "it has never been seriously looked at." The Chairman also questioned the General Accounting Office on this matter and asked if "it would be practical or desirable to institute a system of classifying non-national security information in the government?" Warren Reed's response was positive and expressed support for the concept. He went on to say that:

> As a matter of fact, I believe that is the only mechanism that can be used to decide what the appropriate level of protection required for the information is. And I think it is essential.[94]

In the GAO report "Federal Information Systems Remain Highly Vulnerable to Fraudulent, Wasteful Abusive, and Illegal Practices" GAO made specific recommendations on the concept of classifying non-national security data. With regard to the Chairman's inquiries on classification schemes for non-defense matters Warren Reed in a follow-on letter recommended the following changes:

> Revised Circular A–71, Transmittal Memorandum No. 1, to (1) identify the minimum controls necessary for ensuring a reasonable level of protection over personal, proprietary, and other sensitive information (2) clarify the interrelationship 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 policy and specific guidance for achieving a reasonable level of protection over those systems, using telecommunication networks.
>
> I would like to clarify item (1) above, "identify the minimum controls necessary et cetera." In my opinion, OMB should develop an information classification system similar to that used by the Department of Defense. OMB needs to establish classification categories, such as "nonsensitive," "sensitive," and "sensitive critical," and then specify minimum controls to be applied in each category. For example, in the non-sensitive category, data telecommunications might not require encryption; in the sensitive catgegory, application of the NBS Data Encryption Standard might have to be considered; and in the sensitive-critical category National Security Agency encryption equipment and procedures could be required.
>
> The OMB controls criteria would have to be adjusted by agencies, however, on the basis of risk analysis. For example, an agency might find that a sensitive application does not require encryption because it is transmitted by non-emanating fiber optics. On the other hand, agencies such as FBI and Treasury might find it necessary to increase

[94] Ibid., p. 222.

the controls established for certain sensitive-critical systems.[95]

3. Enhancement of Law Enforcement Capabilities

The complexity and proliferation of modern automated information systems has made investigation into fraud and abuse involving these systems difficult. Computerized resources are dynamic and, in many instances, new technologies change the direction and perspective of a specific system. Therefore it becomes necessary to improve and expand training for those that must detect and prosecute the computer criminal. The FBI reported that their training programs consist of a four-week session, and a condensed version of three-weeks. This training is available to FBI agents, Federal, State and local law enforcement personnel, as well as foreign law enforcement officials. In addition, the FBI indicated that a one week familiarization with computer fraud and computer terminology was given in the field.[96]

Mr. Hancock of the Wells Fargo Bank indicated that there was a need to fund Federal law enforcement activities appropriately in combatting computer crime. He advised that these programs should not only be enhanced but that they might be expanded. Specifically he indicated that:

> . . . we are aware that the Federal agencies such as the Secret Service and the FBI have excellent training programs designed to help their agents detect and investigate computer crime. We would suggest that consideration be given to systematically expanding those programs to permit participation by private sector firms such as banks. This could be accomplished fairly simply by making available appropriate programs through close-circuit television or videofilm. Sharing of appropriate textual materials should be considered.[97]

APPENDIX A. LIST OF WITNESSES

September 26, 1983:
- Neal Patrick, Milwaukee, Wis., accompanied by Paul Piaskoski, Esq., counsel
- Jimmy McClary, division leader for operational security and safeguards division, Los Alamos National Laboratory, Los Alamos, N. Mex., accompanied by Dotty Camillo, group leader, communications and telecommunications group, Los Alamos National Laboratory, N. Mex.
- Donn B. Parker, senior management systems consultant, Informations Systems Management Department, SRI International, Menlo Park, Calif., and Geoffrey S. Goodfellow, senior systems analyst, SRI International, Menlo Park, Calif.
- Stephen T. Walker, president, Trusted Information Systems, Inc., Information Systems Telecommunications, Glenwood, Md.

October 17, 1983:
- Joseph R. Wright, Jr., Deputy Director, Office of Management and Budget, accompanied by John P. McNicholas, Chief, Information Policy, Office of Management and Budget
- Warren Reed, Director, Information Management and Technology Division, U.S. General Accounting Office, accompanied by Walter L. Anderson, Senior Associate Director, Information Management and Technology Division, and Harold J. Podell, Group Director with Information Management and Technology Division
- John W. Lyons, Acting Director, National Bureau of Standards, and Dennis Branstad, Manager, Computer Integrity and Security Technology Group, Institute for Computer Sciences and Technology, National Bureau of Standards, U.S. Dept. of Commerce
- Melville H. Klein, Director, DOD Computer Security Center, National Security Agency, U.S. Department of Defense, accompanied by Col. Roger R. Schell, Deputy Director, DOD Computer Security Center
- Floyd I. Clarke, Deputy Assistant Director, Criminal Investigative Division, Federal Bureau of Investigation, accompanied by Kier T. Boyd, Acting Assistant Director, Technical Services Division, Federal Bureau of Investigation, and Anthony J. Adamski, Jr., Chief, Financial Crimes Unit, Federal Bureau of Investigation
- Richard H. Shriver, Assistant Secretary of the Treasury, Electronic Systems and Information Technology, accompanied by Dr. Bob Conley, Deputy, Advanced Technology; Joe Bishop, Deputy, Programs and Resources Management; and Paul Trause, Inspector General, U.S. Treasury

October 24, 1983:
- Willis H. Ware, information systems, security, and privacy, the Rand Corp.
- Jack L. Hancock, senior vice president, corporate strategy and systems, Wells Fargo Bank
- Julius Cohen, Director of Technology, Information Resource Management Department, Grumman Aerospace Corp.
- Robert Morris, technical staff, Bell Telephone Laboratories, American Telephone & Telegraph Co.
- Elmer I. Clegg, vice president, marketing, Federal Systems Division, Honeywell Information Systems, Inc., accompanied by James I. Bolton, program director, Federal Systems Division, and Paul E. Flaherty, director, software engineering, Federal Systems Division

[95] Ibid., p. 222-223.
[96] Ibid., p. 419.
[97] Ibid., p. 487.

APPENDIX B

LIST OF FEDERAL STATUTES AND EXECUTIVE ORDERS PERTINENT TO SECURITY AND PRIVACY ASPECTS OF COMPUTER RELATED CRIME

Citation	Records affected	Title of the Statute
5 U.S.C. 552	G	Freedom of Information Act.
5 U.S.C. 552a	G	The Privacy Act of 1974.
12 U.S.C. 3401 et seq.	P	Right to Financial Privacy Act.
13 U.S.C. 9214	G	Census Act.
15 U.S.C. 1666a	P	Fair Credit Billing Act.
15 U.S.C. 1681	P	Fair Credit Reporting Act.
15 U.S.C. 1693	P	Electronic Funds Transfer Act.
18 U.S.C. 641	G	Embezzlement and Theft Prohibition.
18 U.S.C. 793, 794	G	Espionage Acts.
18 U.S.C. 1343	G–P	Wire Fraud Prohibition.
18 U.S.C. 1905	G	Trade Secrets Act.
20 U.S.C. 1232g	P	Family Educational Rights and Privacy Act.
26 U.S.C. 6103, 7213, 7216, 7217	G–P	Internal Revenue Code on Confidentiality.
26 U.S.C. 7609	P	Special Procedures for Third Party Summons.
42 U.S.C. 408(h)	G	Confidentiality of Social Security Numbers.
42 U.S.C. 5103(b)(2)(e)	G	Confidentiality of Child Abuse Information.
44 U.S.C. 3101–3315	G	Records Management by Federal Agencies.
44 U.S.C. 3508	G	Interagency Information Exchanges.
E.O. 10865	G	Safeguarding Classified Information Within Industry.
E.O. 12065	G	Rules Governing Classified Information.

Key: G=Government Records Covered. P=Private Sector Records Covered.

Source: U.S. Department of Justice. Bureau of Justice Statistics. Computer Crime: Legislative Resource Manual. Washington, U.S. Govt. Print. Off., 1980. p. 42.