THE JOINT STAFF
WASHINGTON, DC

Reply ZIP Code:
20318-6000

4 July 1996

1. National security in the information age poses significant challenges for the Department of Defense and the nation. All organizations and decision-makers, while embracing the advantages offered by information-based technologies, must respond to the significant vulnerabilities inherent in the systems upon which their capabilities depend. While a growing number of activities are under way to address information assurance needs, more work is needed to advance this issue of growing national importance.

2. In recognition of this need, the Joint Staff commissioned the original version of this study last year to identify and document organizational and other conditions as an educational baseline in the formulation of a comprehensive information protection strategy. That study was extremely well received. Based on that response and the rapid advance of organizational efforts in this dynamic field, we decided to team in updating the study. This document represents the results of that collaboration. As before, the focus is on establishing a current factual baseline to identify the major participants and illuminate key considerations.

3. This product is solely a research effort. Any judgments expressed or implied are those of the study group and should not be interpreted as official Department of Defense positions. We want to express our appreciation to everyone who supported this effort.

4. We would be grateful for feedback regarding this product. If you have any questions or comments regarding this report, please call CAPT Bill Gravell, USN at 703-614-2918, or his lead action officer for this effort, Major Steve Spano, USAF at 703-697-1199. National Defense University points of contact are Dr. John Alger, 202-685-3629, Ext. 365, or Dr. Dan Kuehl, 202-685-3629, Ext. 366.

ARTHUR K. CEBROWSKI
Vice Admiral, USN
Director for C4 Systems

ERVIN J. ROKKE
Lieutenant General, USAF
President, National Defense University

INFORMATION WARFARE

Legal, Regulatory, Policy and Organizational Considerations for Assurance

2nd Edition

4 July 1996

JOINT CHIEFS OF STAFF

NATIONAL DEFENSE UNIVERSITY

"The joint campaign should fully exploit the information differential, that is, the superior access to and ability to effectively employ information on the strategic, operational and tactical situation which advanced US technologies provide our forces."

[Joint Pub 1]

Appendix A Organizational Summaries

Department of Defense

Executive Branch

Interagency Groups

Advisory Committees

Independent Government Corporations

Legislative and Judicial

International, National, State & Local

Points of Contact

Appendix B Reference

U.S. Code

Regulatory

Policy

Additional Resources

References

Acronyms

Glossary

Index

TABLE OF CONTENTS

TABLE OF CONTENTS (Continued)

LIST OF FIGURES

LIST OF FIGURES (Continued)

LIST OF TABLES

This page intentionally left blank.

PREFACE

The performance of essential national security-related functional activities is increasingly dependent on U.S. infrastructures and their supporting information components. In view of the dependency, and because the Department of Defense (DoD) information infrastructure is embedded in larger national and international infrastructures, DoD officials, their advisors, and others within and outside the government have recommended to the National Security Council staff that it may be necessary to initiate interdepartmental/interagency discussions. Topics of such a dialogue would include the dependency and vulnerability issues and the need for national policy to deal with them. The Chief, Information Warfare Division (J6K), Directorate of Command, Control, Communications, and Computer Systems (J6), the Joint Staff, commissioned the original report and this second edition to prepare the Joint Staff to participate in and contribute to these discussions.

The breadth and extreme complexity of the subject matter, other related ongoing activities, and the scope of the task limited the number of environmental areas and organizations which could be addressed. The report does, however, address the breadth and complexity of the policy and strategy issues and summarizes the views of those in positions of importance to the development of policy for infrastructure protection and assurance.

To develop the organizational policy considerations, the study group reviewed organizations that have a stated role in information warfare and organizations that have related missions and functions. This report presents several key organizations in a broad range encompassing international, national, state and local, public and private, and government and industry organizations.

The environmental areas examined were:

- Infrastructures.
- Legal Environment.
- Regulatory Environment.
- Policy Environment.
- Technology Environment.
- Intelligence Environment.

Because of the extensive organizational and reference information documented herein, this report should also be viewed as a source book on background, stakeholders, interests, and activities. This work is expressly intended to build upon, rather than replace, last year's product, the first edition. As a result, much material is repeated from that earlier effort, although this document is one-third larger overall. The sponsors' intentions, then and now, are to present this document to the engaged community as a factual resource, rather than to portray any particular viewpoint, in the interest of building awareness and consensus on required plans and actions. There is still much work to be done—literally every section could be expanded upon in breadth and detail. For the moment, however, we invite the reader to join us as through these pages we move toward the future of national security in the Information Age.

The report is organized as follows:

- Section 1 introduces the report and provides context.
- Section 2 addresses each of the environmental areas noted above.
- Section 3 discusses the methodology of the organizational reviews and provides key findings.
- Section 4 summarizes the findings and observations.
- Sections 1-4 each contain a preview of new material in the section.
- Appendix A identifies organizations which have missions and functions related to defensive information warfare/information assurance. The first page of Appendix A contains an index to the organizations and organizational summaries. Each organizational summary identifies:
  - The organization
  - A senior information official
  - Points of contact
  - On-line resources
  - Information warfare/information assurance related missions and functions
  - Information warfare/information assurance activities, issues, best practices, and lessons learned.

  Each summary also includes a chart that shows the organizational entities which conduct related activities. A consolidated list of points of contact with telephone numbers follows the organizational summaries.
- Appendix B includes:
  - An annotated bibliography of applicable U.S. Code, regulatory documents, and policy documents.
  - References for the report. Citations in the report and in Appendix A are indicated with brackets (e.g., [GAO]).
  - Additional resources related to Sections 2 and 3 of the report.
  - A list of acronyms, a glossary, and an index to the report and to Appendix A.

Information added or significantly changed in this second edition is marked with a vertical line in the margins. Information in this document is current as of July 1, 1996.

WHAT'S NEW?

A short discussion on the *nature of information warfare* has been added.

The discussion on **infrastructures** has been expanded to:

- Discuss U.S. *dependencies on vulnerable infrastructures,* and introduce the concepts of *infrastructure protection* and *infrastructure assurance*,
- Present some *emerging frameworks* for understanding the concepts, and
- Provide additional detail on emerging *information infrastructure assurance activities.*

The **legal environment** section has been revised to:

- *Address new roles, responsibilities, and potential effects* of the Telecommunications Act of 1996, the Kyl Amendment, the Paperwork Reduction Act of 1995, and, the Information Technology Management Reform Act of 1996, and
- Provide additional information about the *Internet and computer crime.*

The **regulatory environment** section has been revised to:

- Include a discussion of *Executive Order 12958, Classified National Security Information*, and provide several additional *Executive Order summaries*,
- Summarize the recently signed *Executive Order 13010 on Critical Infrastructure Protection*,
- Address the *FCC Rule Making impacts* of the Telecommunications Act of 1996 and the infrastructure assurance *implications of the FCC Open Network Architecture.*

The following subjects have been added to the discussion of the **policy environment**: p*olicy development and implementation; risk management; encryption and export policy.*

The discussion of **technology** now provides: some examples of growing dependence on information technology from the *Bosnia experience*; a more detailed examination *of emerging technologies applicable to information assurance*; and information on some of the applicable *research and development activities.*

The **intelligence** (formerly adversary capabilities) section has been enhanced to include material on *threat goals and techniques*, as well as information on *current intelligence community challenges and activities* in information warfare.

In the **organizations** section, *the findings and observations have been updated* from the original report.

On-line resources for additional information on the organizations reviewed have been added to the organizational summaries in **Appendix A**. Appendix A also includes an *improved point of contact listing and a listing of computer emergency response teams.*

A *glossary* and list of *recommended readings and additional resources* keyed to the sections of the report have been added to **Appendix B**.

This page intentionally left blank.

SECTION 1

INTRODUCTION

WHAT'S NEW?

This section now introduces the concepts of infrastructure dependence, infrastructure protection, and infrastructure assurance, and discusses the nature of information warfare.

The national security posture of the United States is becoming increasingly dependent on U.S. infrastructures. These infrastructures are highly interdependent, particularly because of the internetted nature of the information components and because of their reliance on the national information infrastructure. The information infrastructure (which consists of information, information systems, telecommunications, networks, and technology) depends, in turn, upon other infrastructures such as electrical power and other forms of energy.

In recognition of the growing dependency on vulnerable infrastructures over which the government has little control, Department of Defense (DoD) officials, advisory committees, and others have recommended to the National Security Council (NSC) staff the initiation of Federal government interdepartmental discussions of the dependency and vulnerability issues and the possible need for national-level policy to deal with the issues. In addition, as a result of recent acts of terrorism against U.S. government and commercial interests, the President recently signed a policy document [WH 3], which directs the protection of certain critical infrastructures. In addition to the national information infrastructure, each of these critical national infrastructures has a significant information component. Consequently, protection of these infrastructures will depend on protecting the information component of each infrastructure. Actual implementation of the policy will require extensive discussion among numerous communities of interest—national security, law enforcement, the market, and privacy advocates, to name but a few.

A brief review of terms and definitions is appropriate here. The term *defensive information warfare* includes all actions to ensure the availability, confidentiality, and integrity of reliable information vital to national security needs. The term *information assurance* denotes the availability and integrity of information and, for the purpose of this report, is synonymous with defensive information warfare. In general, the term *information warfare* (IW) is used when discussing organizations and activities within the DoD. The term *information assurance* is used when discussing other organizations and activities. The use of the terms *senior information warfare official* and *senior information assurance official* does not imply that there are officially designated positions bearing these titles. These terms indicate a senior official within the organization who has been or might conceivably be assigned the responsibilities for information assurance.

The recently introduced terms *infrastructure protection* and *infrastructure assurance* differ in subtle, yet important, ways. Infrastructure protection is generally considered to mean protection of an infrastructure from physical or electronic attack. Infrastructure assurance includes those actions to achieve surety of readiness, reliability, and continuity of infrastructures such that they are: (1) less vulnerable to disruptions or attack; (2) harmed to a lesser degree in the event of a disruption or attack; and (3) can be readily reconstituted to reestablish vital capabilities. [CIWG]

1.1 PURPOSE

This report documents organizational and environmental considerations which may influence the formulation of information warfare policy and strategy.

1.2 SCOPE

To develop the organizational considerations, the study group reviewed organizations that have a stated role in information warfare or information assurance or that have related missions and functions. The review consisted of research and interviews to identify organizational structures, organizational interests, key individuals (stakeholders) within the organizations, information warfare-related practices, lessons learned, and issues. Figure 1-2-1 shows the types of organizations reviewed. This report presents several key organizations in this broad range.

- ***International***
- ***National***
  - **Public**
    - **Academia**
    - **Public Interest Groups**
  - **Private**
    - **Industries**
    - **Associations**
    - **Alliances**
- ***Federal Government***
  - **Executive Branch**
    - **Department of Defense**
    - **Other Departments**
    - **Interagency Groups**
    - **Advisory Committees**
  - **Independent Establishments and Government Corporations**
  - **Legislative Branch**
  - **Judicial Branch**
- ***State and Local Governments***

Figure 1-2-1. Types of Organizations Reviewed

Figure 1-2-2 shows the environments examined in Section 2. These areas complement ongoing DoD activities that explore other environmental aspects such as requirements, doctrine, training and education, research and development, test and evaluation, and acquisition. Also, at the Federal government interdepartmental level, discussions of information warfare/information assurance issues and the possible need for a national-level policy would center around these environmental areas.

- **Infrastructures**
- **Legal Environment**
- **Regulatory Environment**
- **Policy Environment**
- **Technology Environment**
- **Intelligence Environment**

Figure 1-2-2. Environmental Areas

Because of the responsibilities of the Information Warfare Division of the Joint Staff, this report deals exclusively with defensive information warfare/information assurance issues.

1.3 BACKGROUND

As shown in Figure 1-3-1, Joint Pub 1 advocates the exploitation of the "information differential" in the joint campaign. In exploiting that differential, joint warfighters will depend increasingly upon information and information systems in both offensive and defensive operations. From a defensive information warfare perspective, various individuals, organizations, special studies, and advisory committees have raised concerns regarding the growing dependence of national security upon a vulnerable information infrastructure.

> "The Joint Campaign should fully exploit the information differential, that is, the superior access to and ability to effectively employ information on the strategic, operational, and tactical situation which advanced U.S. technologies provide our forces."

Figure 1-3-1. Joint Pub 1 Quote

During the past three decades, when automated data processing was primarily confined to mainframe computers operating in physically secure facilities, the Congress attempted to define the responsibilities of Federal government organizations and officials for the protection and privacy of information. These attempts notably improved the fields of computer security (COMPUSEC), communications security (COMSEC), and information systems security (INFOSEC) in protecting information and the privacy of individuals.

Still, responsibilities for the protection of the information infrastructure and the privacy of the information contained in the infrastructure have not been well defined. Most of the legislative requirements for the protection and privacy of information apply only to the Federal government.

During this same period, the successful performance of essential economic and national security-related functions became more and more dependent on automated information systems. Banking, retail, telecommunications, and other industries automated operations for cost, competitive, and other reasons. Government and military organizations automated key functional activities to improve response times, save costs, and better meet perceived threats.

Within the last decade, personal computers, workstations, data bases, and mainframes have been interconnected into distributed information networks. This interconnection is continuing at an ever-increasing rate. Through the Internet and other data networks, government networks are interconnected with commercial networks, which are interconnected with military networks, which are interconnected with financial networks, which are interconnected with the networks that control the distribution of electrical power, and so on. It is now almost impossible to distinguish where one network ends and another begins in this extensive and complex information infrastructure.

1.4 THE NATURE OF INFORMATION WARFARE

Information infrastructures are vulnerable to attack. While this in itself poses a national security threat, the linkage between information systems and traditional critical infrastructures has increased the scope and potential of the information warfare threat. For economic reasons, increasing deregulation and competition create an increased reliance on information systems to operate, maintain, and monitor critical infrastructures. This in turn creates a tunnel of vulnerability previously unrealized in the history of conflict. Within the last 2 years, electronic intruders have penetrated major U.S. telecommunications carriers and Internet service providers; many international Post, Telegraph, and Telephone organizations; and a wide variety of end-user systems. [BELLCORE] These intruders have included foreign intelligence agents, economic espionage agents, organized crime members, drug cartel members, private detectives, hackers, and insiders. The nature of information warfare, exemplified by Figure 1-4-1, further complicates information protection/assurance.

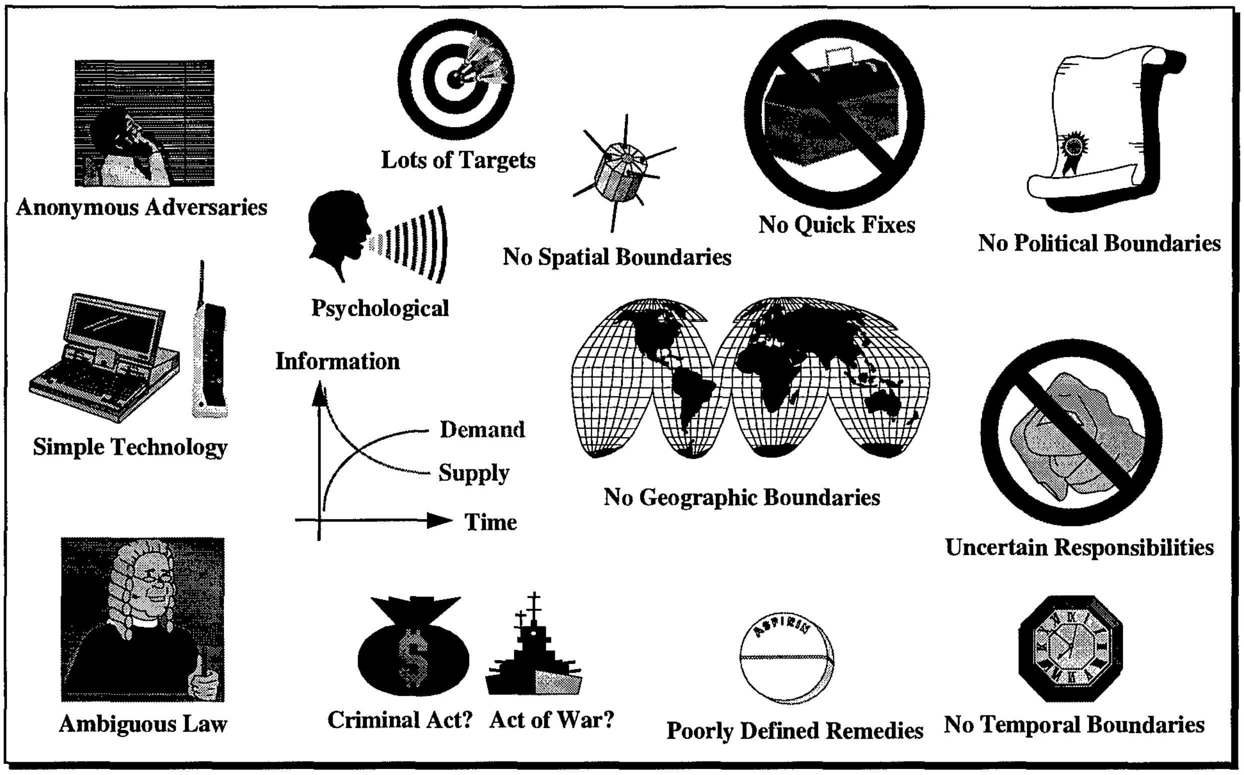


Figure 1-4-1. The Nature of Information Warfare

Information warfare offers a veil of anonymity to potential attackers. Attackers can hide in the mesh of internetworked systems and often use previously conquered systems to launch their attacks. The lack of geographical, spatial, and political boundaries offers further anonymity and legal and regulatory arbitrage; this lack also invalidates previously established "nation-state" sanctuaries. Information warfare is also relatively cheap to wage, offering a high return on investment for resource-poor adversaries. The technology required to mount attacks is relatively simple and ubiquitous. Demand for information will dramatically increase while the capacity of the information infrastructure will decrease relative to demand. The law, particularly international law, is currently ambiguous regarding criminality in and acts of war on information infrastructures. This ambiguity, coupled with a lack of clear designated responsibilities for electronic defense hinders the development of remedies and limits response options. Unless remedied by organizational, legal or regulatory actions, many of these characteristics will be a part of the future reality of IW. In any case, the part that may be brought under control is the assignment of responsibility and authority under law and policy to enhance our position and protect our most vital interests.

This page intentionally left blank.

SECTION 2

ENVIRONMENTAL CONSIDERATIONS

This section discusses the environments within which information warfare must be examined.

Section 2.1 discusses the complex nature of functional activities and the underlying infrastructures upon which they depend. It discusses the nature of the information infrastructure, its vulnerabilities, and some of the ongoing activities to improve the assurance of the infrastructure.

Sections 2.2, 2.3, and 2.4 focus on laws, regulations, and policies most relevant to information assurance—in particular, those that identify key roles, functions and responsibilities. *Public law* applies to all U.S. citizens. It forms the capstone documentation which defines organizations and their responsibilities and which bounds their information warfare/information assurance-related activities. *Regulations* have the full force and effect of law, are associated with permanence, and apply to all U.S. citizens. *Policy* generally applies to some subset of the population and may change with administrations.

Section 2.5 discusses technology in the communications and information security fields and presents the results of recent studies on technologies relevant to information assurance.

Section 2.6 discusses the intelligence environment and some of the challenges faced by the intelligence community.

This page intentionally left blank.

2.1 INFRASTRUCTURES

WHAT'S NEW?

This section now:

- Discusses U.S. dependencies on vulnerable *infrastructures.*
- *Illustrates the vulnerability* with a discussion of the electric power generation and distribution infrastructure.
- Introduces the concepts of *infrastructure protection* and *infrastructure assurance.*
- Presents some *emerging frameworks* for understanding the concepts.
- Provides additional detail on emerging *information infrastructure assurance activities.*

2.1.1 Introduction

This section discusses the complex nature and interdependencies of functional activities and infrastructures (including the information infrastructure and associated telecommunications networks, which serve as the foundation for the other infrastructures and the functional activities they support). This section discusses the nature of these infrastructures, their vulnerabilities, and some of the ongoing activities to improve the assurance of the information infrastructure in particular.

2.1.2 Functional Activities and Infrastructures

The production and delivery of goods and services directly affects the national and economic security of the United States and directly influences the readiness of the military forces. The delivery of these goods and services depends on the complex interactions of various functional activities, industries, commodities, and political, economic, and social conditions.

Consider, for example, the functional activity of deploying a military force from the United States to deal with a regional crisis. This deployment requires moving individual units to ports of embarkation, transporting those units to the region of interest, and employing the force to deal with the crisis. If this deployment involves a sizable force, these activities depend, in turn, on the use of the Nation's transportation infrastructure. Coordinating the activities depends on an effective telecommunications infrastructure. Both the transportation and telecommunications infrastructures depend on the availability of electrical power, which depends on the availability of sufficient energy sources to produce the needed electrical power. Coordinating transportation activities and providing electrical power also depend on an effective telecommunications infrastructure.

Figure 2-1-1 illustrates some components of national and economic security and their possible interactions and interdependencies. [USD(P)] In the figure, the infrastructures shown in white illustrate the interdependencies listed in the example.

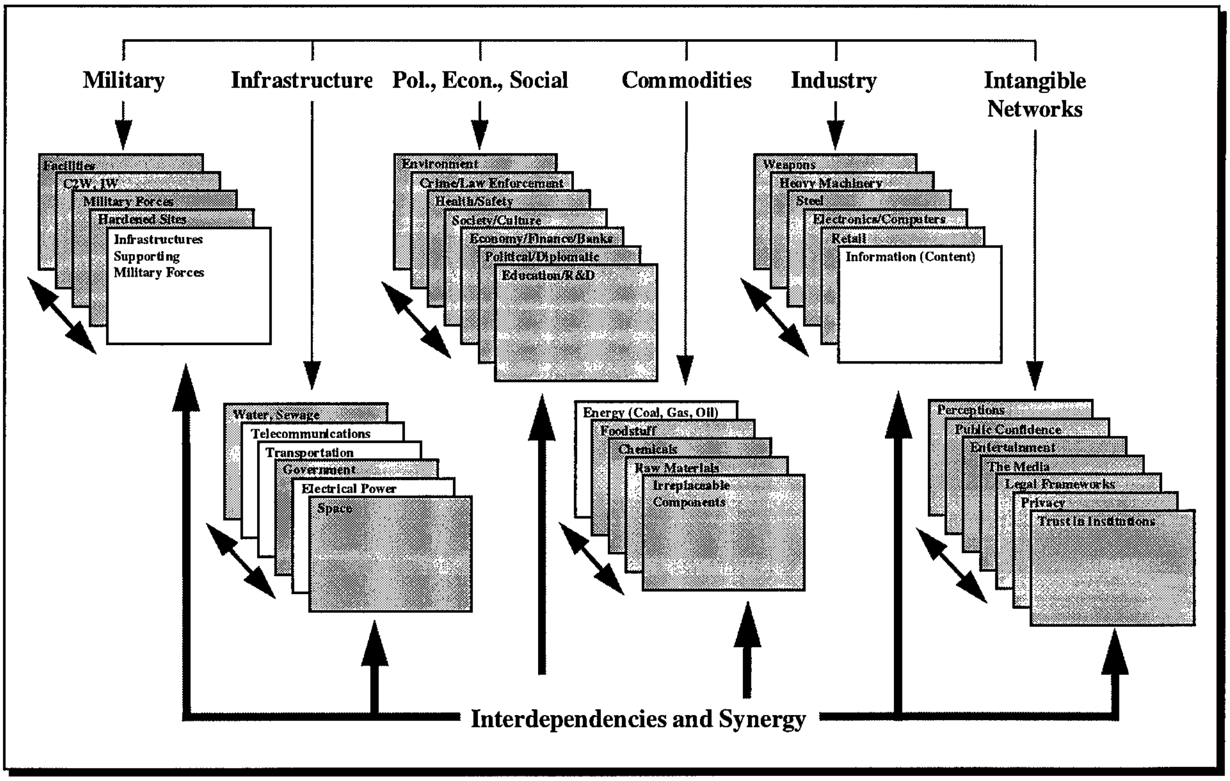


Figure 2-1-1. Components of National and Economic Security

This example forms the basis for several policy questions: What is the legitimate role of the DoD or the Federal government in ensuring the availability of these infrastructures to support critical functions? Who should pay for improvements needed to ensure availability? Who should guide the needed efforts? Because of a growing understanding of infrastructure dependencies, these and many similar policy questions are now being asked. While this report does not answer the questions, it does explain some of the complexities of the problem, in the hope of facilitating discussions which will lead to the answers.

In general, U.S. infrastructures are extremely reliable and available because they have been designed to respond to disruptions, particularly those caused by natural phenomena. Redundancy and diverse routing are two examples of design techniques used to improve reliability and availability. However, deregulation and increased competition cause companies operating these infrastructures to rely more and more on information technology to centralize control of their operations and to provide service to their customers. This centralization and the increased reliance on broadly networked information systems increase the vulnerabilities of the infrastructure and the likelihood of disruptions or malevolent attacks. A brief discussion of the electric power generation and distribution infrastructure will illustrate some of these points.

2.1.3 Electric Power Generation and Distribution Infrastructure

Electric power is produced by generating plants and delivered to customers via the transmission, subtransmission, and distribution systems. *Interties*, or transmission lines and control lines, interconnect adjoining power systems and control areas. Most utilities employ a primary and a back-up control center. The control centers monitor the generating plants, the transmission and subtransmission system, interties, the distribution system, and, in some cases, customer loads or service entrances. Distribution control centers are used in very large utilities to control portions of the subtransmission and distribution facilities. In some cases, control centers are established by regional power pools formed for the purpose of sharing loads and providing additional generation capacity. In general, control of the infrastructure is exercised at the local level (e.g., circuit breakers at the generators), at the utility level (e.g., the central control center), and at the regional power pool level.

The basic structure of an electric power system is shown in Figure 2-1-2.

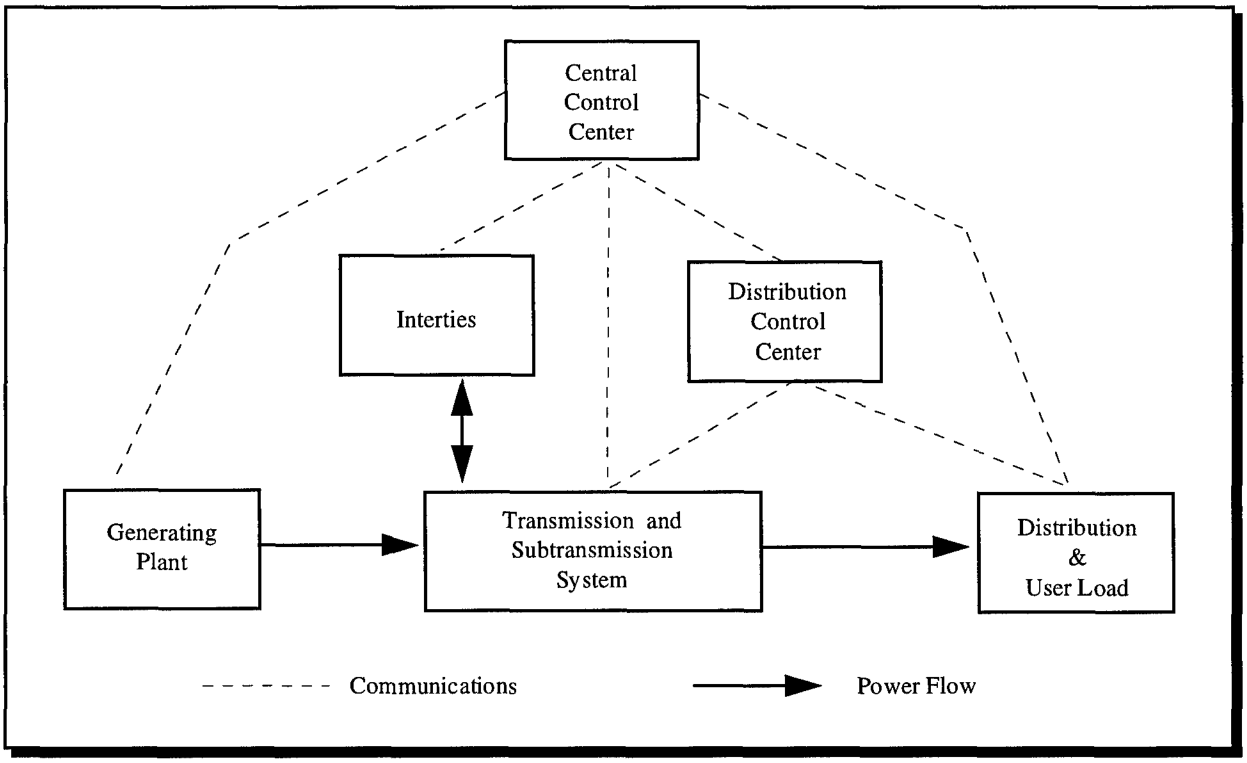


Figure 2-1-2. Electric Power System

Electric utilities devote significant resources to applying centralized automation technology involving the extensive use of high-speed digital computers, supervisory and control systems, communications systems, and telemetering systems. Figure 2-1-3 illustrates a typical central control center configuration.

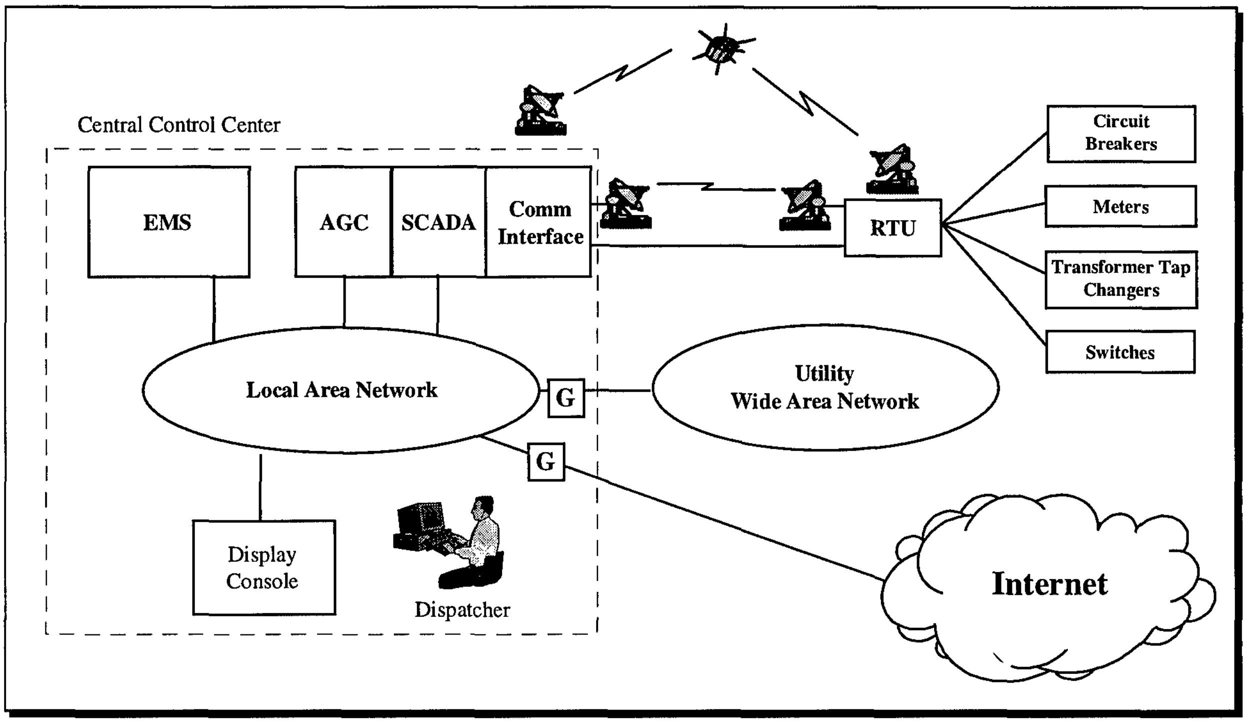


Figure 2-1-3. Typical Central Control Center Configuration

The Energy Management System (EMS) is the heart of the control center operation. It consists of computer hardware, operating systems, and applications for many functions such as on-line power flow, generator scheduling, load forecast, load management, frequency control, and the like. The Supervisory Control and Data Acquisition (SCADA) system serves as the interface between the remotely monitored and controlled devices of the power system, the EMS, and the control center personnel. In some newer applications, EMS and SCADA are being combined and use a common operating system and data bases.

The SCADA system polls the remote terminal units (RTU) for status information (e.g., voltage, frequency, phase angles, power flow, alarms) and passes status information to the EMS. The status information is processed by the EMS and displayed on the dispatcher's console. The dispatcher may elect to take corrective action such as opening circuit breakers or switching loads. These action commands are transmitted by the SCADA system in the form of control signals to the appropriate RTU which, in turn, converts the control signals into the form necessary to manipulate the appropriate devices. In cases requiring rapid intervention, the EMS initiates controls signals without dispatcher intervention.

The Automatic Generation Control (AGC) provides supplementary control functions to generating units to meet economic and load-frequency criteria of the power system and based on the scheduling, forecasting, and analysis performed by the EMS.

The communications interface links the SCADA with the various communications media used to transmit the status and control signals. These communications media include microwave radio, fiber-optic networks, dedicated and leased lines, satellite radio, and the public switched network in general order of prevalence. In addition, some utilities use a Power-line Carrier (PLC) technology which enables the transmission of very low frequency (and low bandwidth) signals over the electrical transmission and distribution conductors. A local area network (LAN) interconnects the EMS, AGC, SCADA, and display consoles. In many cases this LAN is connected through a gateway (G) to a utility wide area network (WAN).

Because of deregulation and increased competition, the power industry is moving more and more toward the use of open systems, standard protocols, and home-based access for maintenance during evening hours, using remote access to LANs. Because of recent Federal Energy Regulatory Commission rulings on equal transmission access for power generation entities, a growing number of power providers, transmission providers, and users are using the Internet-based Open Access Same Time Information System (OASIS) to advertise and purchase power and transmission capability. [KEMA-ECC]

The Information Science and Technology (ISAT) 1995 Summer Study on Survivable Distributed Information Systems included a case study on the electric power generation and distribution infrastructure. [DARPA] The study team found that commercial LANs and workstations are used throughout the infrastructure and that more and more utilities are employing modern open-system architectures and standardized public protocols. The team also found security loopholes in the form of Internet connectivity and dial-in modem ports for maintenance operator access to the control system LAN. The study team postulated a possible attack scenario and resultant disruption. The threat of such an attack is very low, however; a successful attack would require fairly detailed knowledge of the SCADA and EMS systems and protocols.

The information and control component of the power generation and distribution infrastructure is very similar to that of other infrastructures. The gas and oil storage and distribution infrastructure also uses the SCADA system and protocols extensively. The complexity of the information component of these infrastructures, however, pales in comparison to the complexity of the transportation and finance and banking infrastructures.

This section is based on the work of the Joint Program Office for Special Technology Countermeasures. [JPO 1]

2.1.4 Infrastructure Protection

As a result of the growing dependencies on information technology, the centralization of control, and the recent acts of terrorism directed against government and commercial interests within the United States, in late 1995 the President signed Presidential Decision Directive (PDD) 39. This directive protects certain critical infrastructures. Infrastructures such as those associated with transportation, power generation and distribution, and national information, are considered critical because they support the national and economic security interests of the United States. The DoD, in particular, depends heavily on these infrastructures. Each of these critical infrastructures has a significant information component. Protecting the infrastructure will depend on protecting the information component.

Protection against physical and electronic attacks and ensuring the availability of the infrastructures will be complicated. These infrastructures are provided mostly (and in some cases exclusively) by the commercial sector; regulated in part by federal, state, and local governments; and significantly influenced by market forces. Commercial services from the national information infrastructure provide the vast majority of the telecommunications portion of the DII. These services are regulated by Federal and state agencies. Local government agencies regulate the cable television portion of the information infrastructure. Power generation and distribution are provided by very diverse activities—the Federal government, public utilities, cooperatives, and private companies. Interstate telecommunications are regulated by the Federal Communications Commission, intrastate telecommunications by the state public utilities commissions. Interstate power distribution is regulated by the Federal Energy Regulatory Commission, intrastate power generation and distribution by the state public utilities commissions.

To add to this confusion, the Telecommunications Act of 1996 decreases regulation of the industry and encourages the eventual entry of long-distance telecommunications, local telecommunications, and cable television service providers into each other's markets. This deregulation will increase competition and reduce the cost of services. Power industry utilities, for example, are very interested in using their extensive rights-of-way to homes and businesses to leverage their entry into the telecommunications market. Utilities are already testing these concepts, introducing several new players into the telecommunications infrastructure.

There are, however, several factors influencing infrastructure assurance. The most significant of these factors is the market. Competitors providing services within an infrastructure will invest to ensure robust and reliable service, but only to the extent necessary to retain or grow market share. Regulation of service providers within an infrastructure is generally undertaken to ensure safety and availability of service or to control the price of the service. Potential liability is another factor which influences a service provider to ensure robust and reliable service. It is interesting to note, however, that an acknowledgment of infrastructure vulnerabilities increases the potential liability of a service provider; the service provider is less likely to acknowledge or share information about those vulnerabilities.

The interaction of these market, regulatory, and potential liability forces in an environment of rapid change (such as the telecommunications market) cannot be predicted, let alone fully understood. It is important, however, to recognize the potential influence of these forces in determining infrastructure protection strategies for the near future.

2.1.5 Infrastructure Assurance

Infrastructure assurance differs from infrastructure protection in subtle, yet important, ways. *Infrastructure protection* means protection of an infrastructure from physical or electronic attack. *Infrastructure assurance* includes those actions needed to ensure readiness, reliability, and continuity of infrastructures. These actions make the infrastructure less vulnerable to disruptions or attack; restrict damage in the event of a disruption or attack; and enable the infrastructure to be readily reconstituted to reestablish vital capabilities. [CIWG]

Translating the concept of infrastructure assurance into an understanding of reality requires some framework for relating the conceptual actions to ongoing actions in "the real world." One such emerging framework is the infrastructure assurance model. This model is based on a recently promulgated policy document, CJCSI 6510.01A, Defensive Information Warfare Implementation [CJCS]. Similar concepts are also found in a draft management plan [DISA] and some of the preliminary activity of the Defense Science Board Task Force on Information Warfare Defense.

The infrastructure assurance model (or framework) consists of the following functional requirements: *deter* information warfare; *protect* the infrastructure from disruptions, intrusions, and attack; provide *indications and warning* of strategic threats to the infrastructure, *detect* disruptions of, intrusions into, and attacks against the infrastructure; *restore* services; and initiate the *response* process. In general, deter and protect are preparedness requirements. Detect, restore, and respond are operational requirements. Infrastructure assurance is a balanced investment in meeting these requirements so as to "achieve surety of readiness, reliability, and continuity of infrastructures."

In the information age as in the nuclear age, *deterrence* should be the first line of defense. Technology to conduct information warfare is simple and ubiquitous; some form of protection is essential. It is technically and economically impossible to fully *protect* the infrastructure (or avoid all risk). The risk can be managed, however, by protecting selected portions of the infrastructure that support functions and activities necessary for maintaining national economic and security interests. To ensure the continuance of these critical functions and activities in the presence of disruptions or attacks requires the detection of disruptions, intrusions, and attacks. Since the information components of the infrastructures are extensively interconnected, an intrusion into or attack against one portion of the overall infrastructure might well cascade into other parts of the infrastructure or into other infrastructures. Consequently, there is a need to contain the "battle damage," prevent cascading effects, and *restore* the infrastructure to its full-service capabilities. Finally, some form of *response* to the intrusions or attacks may be necessary to deter future intrusions or attacks. Because response could involve some form of offensive information warfare, it will not be addressed in any significant detail in this report.

Table 2-1-1 and Figure 2-1-4 further describe the infrastructure assurance model.

Table 2-1-1. Infrastructure Assurance Model

Deter	• **Address international issues.** • **Enact necessary legislation**. Actively **enforce the law.** • **Implement required regulations.** • **Promulgate clear policy**. • **Institute awareness, training, and education programs.** • **Establish management controls.** • **Coordinate efforts.** • **Allocate necessary resources.** • **Develop an effective protect, detect, restore and response capability**.
Protect	• **Develop and implement plans** for a protected information environment (risk management). – Analyze the risk (objects, vulnerabilities, threat, impact). – Identify risk reduction possibilities. – Get management decision on acceptable risk. – Develop risk reduction plan (scope and standards for protection). – Develop, implement, and maintain safeguards. – Test, review, and audit safeguards. • **Employ advanced technology**.
I&W	• **Provide needed strategic intelligence support.** • **Provide needed C4 for dissemination of strategic warning.**
Detect	• **Provide near real-time detection** of disruptions, intrusions, attacks. • **Share sensitive information (threats, vulnerabilities, intrusions, attacks)** - competing interests: intelligence, law enforcement, the market, privacy. • **Conduct exercises.**
Restore	• **Assess “battle damage”** - determine nature and extent of damage to formulate tactical warning and establish reallocation and restoration priorities. *(Part of Attack Assessment)* • **Warn users and operators**. *(Tactical Warning)* • **Isolate and contain the “battle damage.”** • **Reallocate key infrastructure capacity** and services to critical functions and activities. *(Continuity of Operations)* • **Restore the infrastructure** to its full operational capability.
Respond	• **Ascertain the nature, severity, sponsorship, complicity of attacks** (acts of war) for proper response. *(Attack Assessment)* • **Explore the range of options**: – Civil prosecution. – Criminal prosecution. – Military force. – Informational persuasion. – Diplomatic action. – Economic mandates. • **Use direct action or perception management.** • **Restore deterrence** based on credible, flexible, and alert defenses.

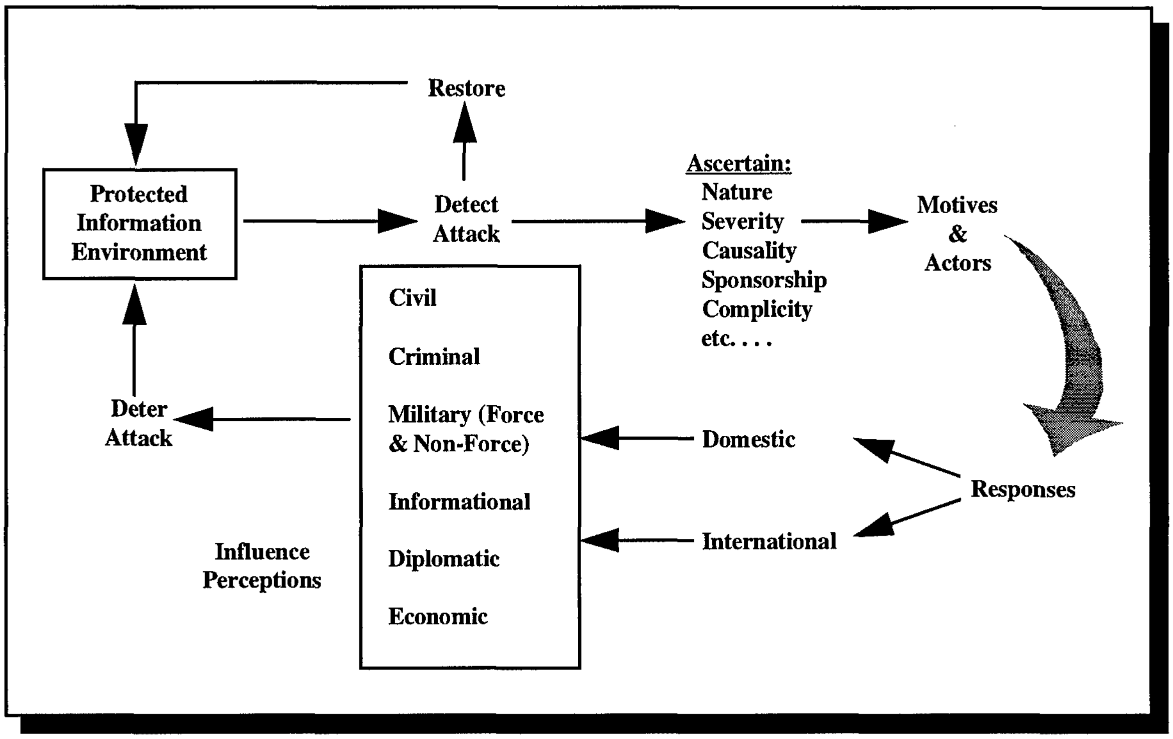


Figure 2-1-4. Infrastructure Assurance Model

The model is scalable and infrastructure independent. It can be applied equally well to a local area network environment or to a natural gas distribution network. The table includes references to indications and warning, attack assessment, tactical warning, and continuity of operations. These terms are military terms which are explained in the glossary. They are included to aid in understanding of the model. It should also be noted that indications and warning is traditionally a strategic intelligence function, while the remainder are operations functions. Section 2.6, Intelligence Environment, discusses the difficulty of conducting intelligence collection and fusion to permit strategic indications and warning.

Figure 2-1-5 provides a view of the critical infrastructures and some of the organizations which are involved in infrastructure assurance through oversight, providing emergency services, regulation, and market-driven operation of the infrastructures. The figure provides a framework for understanding the complexity of infrastructure assurance, emphasizes the number and diversity of organizations involved, and, for the telecommunications infrastructure, shows some of the ongoing infrastructure assurance activities.

The top layer includes the Executive Branch departments and organizations involved in developing policy and procedures, along with some subordinate departmental organizations with oversight or regulatory responsibilities. The next layer of organizations includes a representative sampling of the Independent Establishments and Government Corporations. These organizations are, for the most part, created by the Congress for regulatory control. The critical infrastructures are shown as elongated rectangles in the lower right portion of the figure. Note that one of the infrastructures is telecommunications, the foundation for the larger information infrastructure. These infrastructures are arrayed under those Executive Branch departments, Independent Establishments, and Government Corporations which have some specified oversight or regulatory control over the infrastructures. [USGM]

The Federal Response Plan outlines responsibilities for various agencies in responding to natural disasters, technological emergencies, and other incidents requiring Federal assistance. [FEMA] Because of the relation between these disaster and emergency situations and infrastructure assurance, it is important to note which agencies have responsibilities under the Federal Response Plan for the critical infrastructures. (For more information on the Federal Response Plan, see the reference or the organizational summary for FEMA in Appendix A.) Advisory, operations, and infrastructure assurance activities are shown in the lower left portion of the figure. In some cases, associations play a role in infrastructure assurance. For example, the North American Electric Reliability Council (shown at the bottom of the figure) is an association of electric utilities which develops technical operating standards for the electrical power infrastructure. Some of the involved organizations and infrastructure assurance activities are shown for the telecommunications infrastructure. Section 2.1.8 outlines some of these activities. The acronym listing and the index also provide more detail about these organizations and their activities.

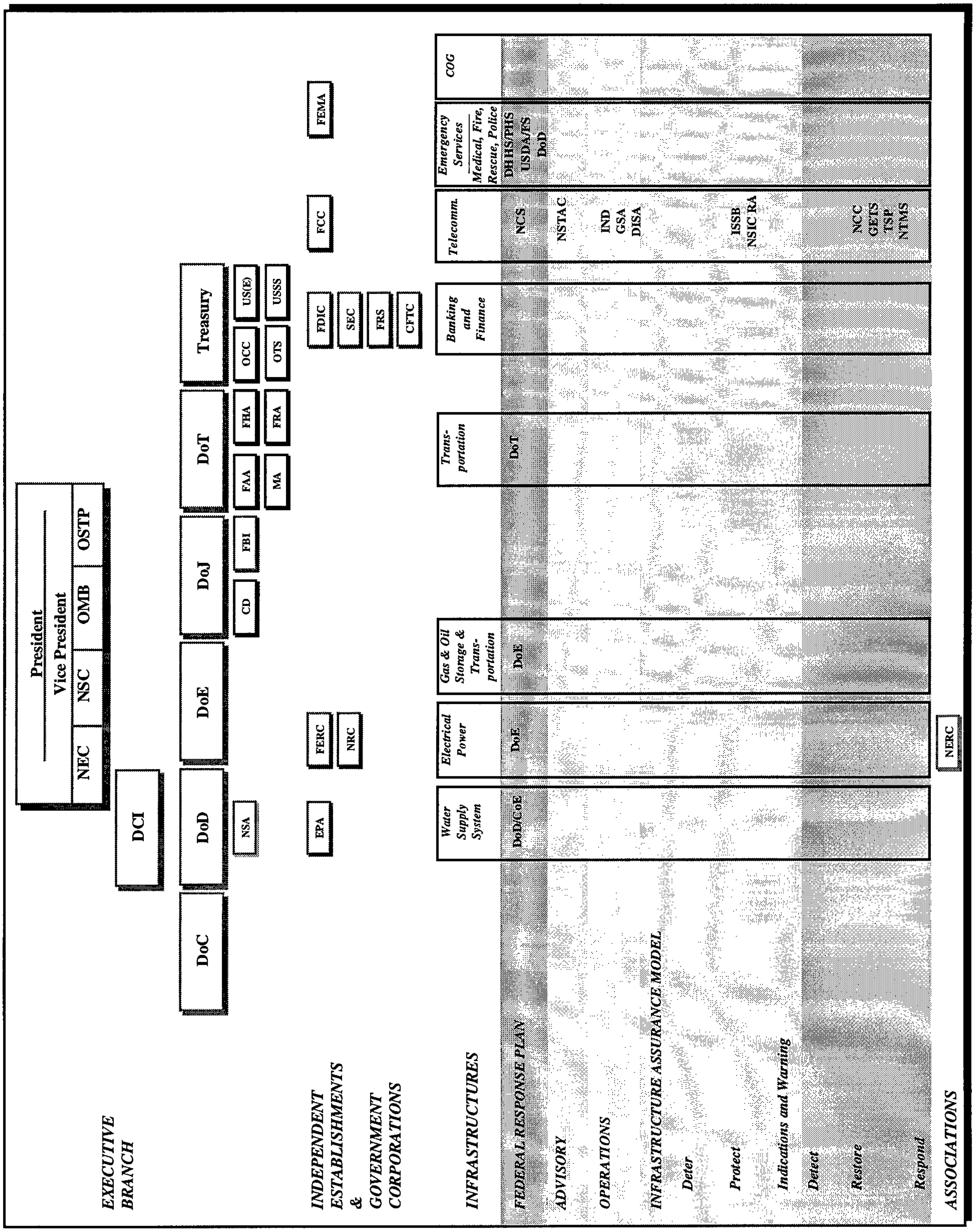


Figure 2-1-5. Critical Infrastructure Protection

As suggested in Table 2-1-1, one of the key first steps in infrastructure assurance is that of risk analysis. Several recent studies [DARPA] [JPO 2] [NSTAC 1] [RVWG] and some planned studies [CIWG] [JS] [NSTAC 2] include some risk analysis. Table 2-1-2 shows the infrastructures of interest in these studies. The table indicates the diversity of interest, lack of consistent definition, and variety of activities involved in the infrastructures. Some of these infrastructures are consumer oriented; others are generation and distribution oriented. It is not possible to postulate overlap in effort because of differences in approach, methodology, and purpose of the studies.

Table 2-1-2. Infrastructure Risk Analysis Activities

	[CIWG]	[DARPA]	[JPO 2]	[JS]	[NSTAC 1]	[NSTAC 2]	[RVWG]
INFRASTRUCTURES							
Banking and Finance	X	X				X	
Education							X
Electric Power	X	X	X			X	
Emergency Services	X						
Energy				X			
Energy Distribution & Supply							X
Entertainment							X
Financial							X
Gas and Oil Storage & Trans.	X						
Government Operations	X						
Health Care							X
Information				X			
Information Distribution							X
Intelligence				X			
NS/EP & Public Safety							X
Telecommunications	X	X	X	X	X	X	
Transportation	X		X	X		X	X
Water Supply	X						

The remainder of the report will focus on the information infrastructure.

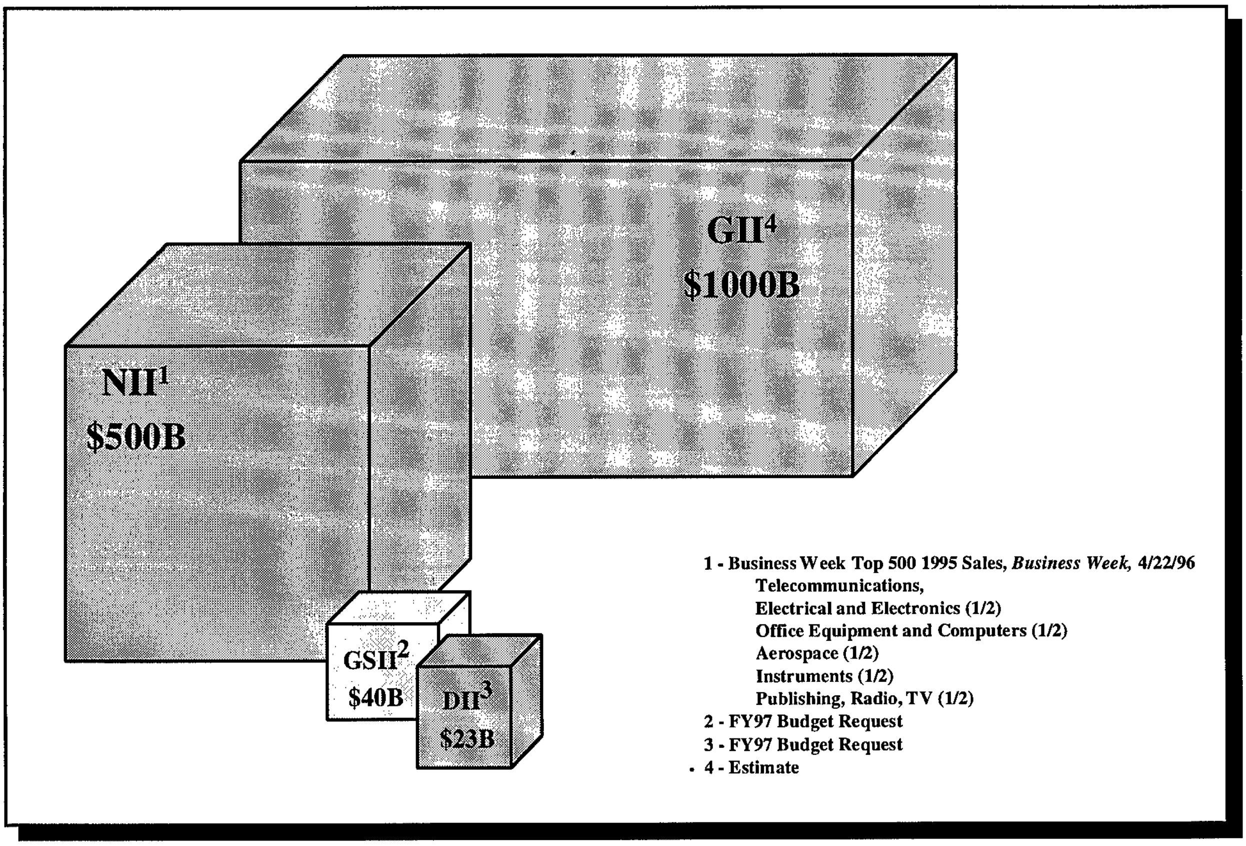
2.1.6 Nature of the Information Infrastructure

Most economic and national security functional activities use the information infrastructure, and in particular the telecommunications networks. In the private sector, these economic activities include such actions as governing, banking, and manufacturing in the private sector. In the national security environment, these activities might include transportation, logistics, pay and other monetary disbursements, manpower and personnel actions, and training.

The information infrastructure supports all of these activities, and it is difficult to distinguish which portions of the infrastructure support which functional activities. Therefore, this discussion will address the general nature of a singular, total information infrastructure, its vulnerabilities, and some of the activities under way to improve the assurance of the infrastructure.

The information infrastructure is extremely complex. There is no simple way to define it, to establish its bounds, to measure its impact, or to identify clear responsibilities for the evolution, operation, maintenance, and repair of the infrastructure. Therefore, the various views of the infrastructure presented by this report only partially address the complexity.

While it is not possible to accurately estimate the size or value of infrastructures, a rough estimate can be made based on trade press estimates, federal budget requests, and other such sources. Figure 2-1-6 shows the estimated relative size of the Global Information Infrastructure, the National Information Infrastructure, Government Services Information Infrastructure (Federal government only), and the Defense Information Infrastructure. It is clear that the DoD and the Federal government are not sizable market forces and, therefore, not capable of solely or significantly influencing the direction (and assurance) of the information infrastructure on a purely economic basis. Public policy will be necessary as a supplement to market forces to define, achieve, and maintain the required levels of assurance.



1 - Business Week Top 500 1995 Sales, *Business Week*, 4/22/96
Telecommunications,
Electrical and Electronics (1/2)
Office Equipment and Computers (1/2)
Aerospace (1/2)
Instruments (1/2)
Publishing, Radio, TV (1/2)
2 - FY97 Budget Request
3 - FY97 Budget Request
4 - Estimate

Figure 2-1-6. Information Infrastructures in Perspective

One way of viewing the information infrastructure is in terms of its basic components. In very simple terms, the information infrastructure comprises the components necessary for the transmission of information, the information itself, the means for creating, gathering, and processing data to obtain information, and the storage of the data and information. In the broadest sense, the infrastructure consists of data, information, equipment, facilities, telecommunications, and people. Table 2-1-3 provides examples of typical information infrastructure components. [IITF]

Table 2-1-3. Typical Information Infrastructure Components

- **Cameras**
- **Scanners**
- **Keyboards**
- **Telephones**
- **Fax Machines**
- **Computers**
- **Switches**
- **Compact Disks**
- **Video and Audio Tape**
- **Cable**
- **Wire**
- **Satellites**
- **Optical Fiber**
- **Microwave Nets**
- **Switches**
- **Television**
- **Monitors**
- **Printers**

Another way of viewing the information infrastructure is as a collection of various networks and services. Some of these networks and services, such as the Internet and the public switched telephone and public data networks, have an identity of their own and are clearly an integral part of the information infrastructure. Others, such as the financial networks and services, have been developed within a specific industry and have evolved into a complex integrated networks necessary to provide responsive support to the customer. Table 2-1-4 shows some of these networks and services.

Table 2-1-4. Typical Information Infrastructure Networks and Services

- **Internet**
- **Public Switched Telephone Network**
- **Public Data Networks**
- **Cellular Networks**
- **Commercial Satellite Networks**
- **Broadcast Radio Networks**
- **Broadcast TV Networks**
- **Cable TV Networks**
- **Defense Data Network**
- **Encryption**
- **Direct Broadcast Satellite (TV)**
- **On-line Services**
- **Publishing Services**
- **Entertainment Services**
- **Financial Networks and Services**
- **Power Networks**
- **Transportation Networks**
- **Public Safety Networks**
- **FTS 2000**

The information infrastructure can also be thought of in terms of the various domains it serves. Table 2-1-5 shows some of these domains. In reviewing the table, it should be evident that the infrastructure contains a vast amount of sensitive information.

Table 2-1-5. Typical Information Infrastructure Domains

- **News**
- **Health and Safety**
- **Navigation**
- **Weather**
- **Government**
- **Transportation**
- **Entertainment**
- **Intelligence**
- **Military**
- **Law Enforcement**

The information infrastructure should also be considered in terms of the stakeholders with an interest in the future evolution of infrastructure. Table 2-1-6 shows some typical stakeholders. The military needs an extremely reliable and robust infrastructure to ensure the availability of critical information during times of crisis. U.S. citizens insist on protection of their individual rights, particularly the right to privacy. On the other hand, sellers of information content insist on universal service to increase their market.

Table 2-1-6. Typical Information Infrastructure Stakeholders

- **Federal government**
- **Military**
- **The Economic Marketplace**
- **Industries**
- **Industry Alliances**
- **Congress**
- **State Governments**
- **Regional Governmental Alliances**
- **Public Servants**
- **Academia**
- **International Economic Groups**
- **International Political Groups**
- **Labor Organizations**
- **Local Governments**
- **Public Interest Groups**

The infrastructure will be shaped by the interests of these stakeholders. For example, the Federal government may seek to intervene in the evolution of the infrastructure for national security and other considerations. Table 2-1-7 shows some of the typical stakeholder interests which may be unique to individual stakeholders or shared by groups of stakeholders.

Table 2-1-7. Typical Information Infrastructure Stakeholder Interests

- **Universal Service**
- **Information Assurance**
- **Intellectual Property Rights**
- **Interconnection**
- **Interoperability**
- **Ownership**
- **Pricing**
- **Jobs**
- **Regulation**
- **Privacy (Security)**
- **Spectrum Management**
- **Standards and Protocols**
- **Technologies**
- **User Education about Vulnerabilities**
- **User Friendly Interfaces**
- **National Security**

It should be clear that there is no single view of the information infrastructure, nor is there a simple way of understanding its complexity. The evolution of the infrastructure (past, present, and future) was, is being, and will be formed by a multitude of competing interests and technologies. Access to the infrastructure is essentially unlimited. Access to the sensitive information located throughout the infrastructure is not well managed. For example, recent tests by the Defense Information Systems Agency (DISA) revealed that 65 percent of targeted computers could be penetrated, only 4 percent of the successful penetrations were detected, and only 27 percent of the detections were reported. [GAO]

2.1.7 Information Infrastructure Vulnerabilities

The information infrastructure is vulnerable to many disruptive forces including natural events, mistakes, technical failures, and malicious acts:

- A lightning strike on a critical node in a network may cause node failure; an earthquake or hurricane may not only physically disrupt the network but also cause network congestion, another source of disruption.
- Inadvertently erasing a data base containing terrain data critically needed for a cruise missile strike may compromise a key part of an offensive strike.
- Cutting a fiber-optic cable with a backhoe may result in the loss of a primary telecommunications link.
- Power failure at a critical network node may cause a significant loss of data and information and may isolate portions of the network.
- Corruption of key network management data by a network manager can cause many networks to fail.
- Viruses introduced by an enemy agent located in a safe haven can cause a network to become overloaded and ineffective or to break down at a critical juncture.

The disruptive nature of such occurrences, whether maliciously or unintentionally caused, was demonstrated in 1988, when a software worm released into the Internet infected over 6000 host computers worldwide in less than 2 hours, and in 1991, when the near-total shutdown of telephone service in the Baltimore-Washington area was caused by a one-byte coding error—a "d" was replaced with a "6."

Over the past two years, unknown intruders have penetrated major U.S. telecommunications carriers, major Internet service providers, many international Post, Telegraph, and Telephone entities, and a wide variety of end-user systems. Targets of these intrusions have included those shown in Table 2-1-8. [BELLCORE]

Table 2-1-8. Targets of Intrusions

- **Service Control Points**
- **Signal Transfer Points**
- **Network Elements**
- **Network Element Managers**
- **X.400 Gateway Systems**
- **Billing Systems**
- **Provisioning Systems**
- **Loop Maintenance Systems**
- **Document Support Systems**
- **X.25 Packet Data Networks**
- **Digital Cross Connect System**
- **Research and Development Systems**

Given the extreme dependence of our national and economic security upon the information infrastructure, it is prudent to assume that the infrastructure will be the target of an information warfare attack. According to Sun Tzu, "It is a doctrine of war not to assume the enemy will not come, but rather to rely on one's readiness to meet him; not to presume that he will not attack, but rather to make one's self invincible."

Section 2.6 discusses possible adversaries in any such attacks. These attacks may take several different forms:

- Physical (electrical and other) attacks on infrastructure components such as computers, communications, software, data, cables, and the control process.
- Physical attacks on infrastructure support such as buildings, power, and environmental control units.
- Physical attacks on or subversion of operating and support personnel.
- Logic (software) attacks on infrastructure components.
- Logic attacks on computer-controlled environmental control units.
- Combined physical and logical attacks to mask one or the other.
- Logic attacks on data (destruction or disruption).

If the infrastructure is directly attacked, it is not known which portions of the infrastructure will be affected, or what effect the loss of portions of the infrastructure will have on the performance of essential functional activities. Because of the extensive internetworking, the second- and higher order effects (e.g., trust and confidence in the infrastructure) of such attacks cannot be predicted. These areas require study and research.

2.1.8 Information Infrastructure Assurance

Information infrastructure assurance is not necessarily a new concept. During the Cold War, the DoD (and the Federal government) took extraordinary steps and made significant investments to ensure the survivability of the telecommunications infrastructure. The Minimum Essential Emergency Communications Network and the Milstar program are two of many examples. While the principles of assurance have not necessarily changed, the environment has changed enormously. The DoD can no longer afford to operate self-contained systems and networks. Distinguishing between telecommunications and information systems and processes is becoming more and more difficult. Everything is interconnected, which means nearly everyone has a vested interest.

Information infrastructure assurance will not be easy to achieve. Given the dependence of the DII on the national information and power generation and distribution infrastructures, assuring the availability of DII services will be an equally difficult endeavor. However, several efforts are under way to address many of these issues. It is not within the scope of this report to describe all of these activities in exhaustive detail. The following paragraphs, however, provide a sampling of these activities from a DoD, a Federal government, and a national-level perspective.

Several offices within the Office of the Secretary of Defense (OSD) and the Joint Staff are assessing infrastructure reliability, including net assessments, policy reviews, assessments of current and planned programs, and a National Defense Infrastructures Survivability Study.

Among the Defense Agencies, Defense Information Systems Agency (DISA) is primarily responsible for protecting the DoD portion of the information infrastructure. DISA has published documents related to the protection of the Defense Information Infrastructure and intends to expand its Defensive Information Warfare (IW-D) Management Plan to include related Service and Agency plans. The National Security Agency (NSA) has research and development activities under way in the area of INFOSEC. The Defense Advanced Research Projects Agency (DARPA) recently combined two primary research areas, one in the IW-D area and one in the INFOSEC area, into an Information Survivability Program. These DARPA research activities will deal with selected information infrastructure vulnerability and reliability issues and, to the extent possible, will be conducted on a cooperative basis with industry. Finally, the Defense Science Board Task Force on Information Warfare Defense will report its findings and recommendations in late summer of 1996. It is expected that the DSB Task Force will make several recommendations regarding the establishment of organizations charged with collecting and sharing sensitive information on NII and DII operations, threats, vulnerabilities, intrusions, and attacks.

From a Federal government perspective, PDD 29, signed in the latter part of 1994, created the Security Policy Board. This Board addresses a variety of security issues, including information systems security and risk management. [WH 2] The Security Policy Board considers, coordinates, and recommends for implementation to the President, through the Assistant to the President for National Security Affairs, policy directives for U.S. security policies, procedures, and practices. The Security Policy Board is the principal mechanism for reviewing and proposing to the NSC legislative initiatives and executive orders pertaining to U.S. security policy, procedures, and practices that do not fall under the statutory jurisdiction of the Secretary of State. This Board coordinates the development of interagency agreements and resolves conflicts that may arise over the terms and implementation of these agreements. In coordinating security policy, procedures and practices, the Policy Board ensures that all U.S. Departments and Agencies affected by such decisions are allowed to comment on such proposals.

PDD 29 also established a Security Policy Advisory Board to serve as an independent, non-governmental advisory body. Five members, including a Chairman, will be appointed by the President for terms of up to 3 years. As of June, 1996, the Chairman and two members have been appointed and are being briefed in preparation for their first meeting. The Chairman will report annually to the President through the Assistant to the President for National Security Affairs on the implementation of the four policy principles, as shown in Figure 2-1-7. The Security Policy Advisory Board will also provide a non-governmental and public interest perspective on security policy initiatives to the Security Policy Board and the intelligence community.

Figure 2-1-7 also shows membership and organization of the Board.

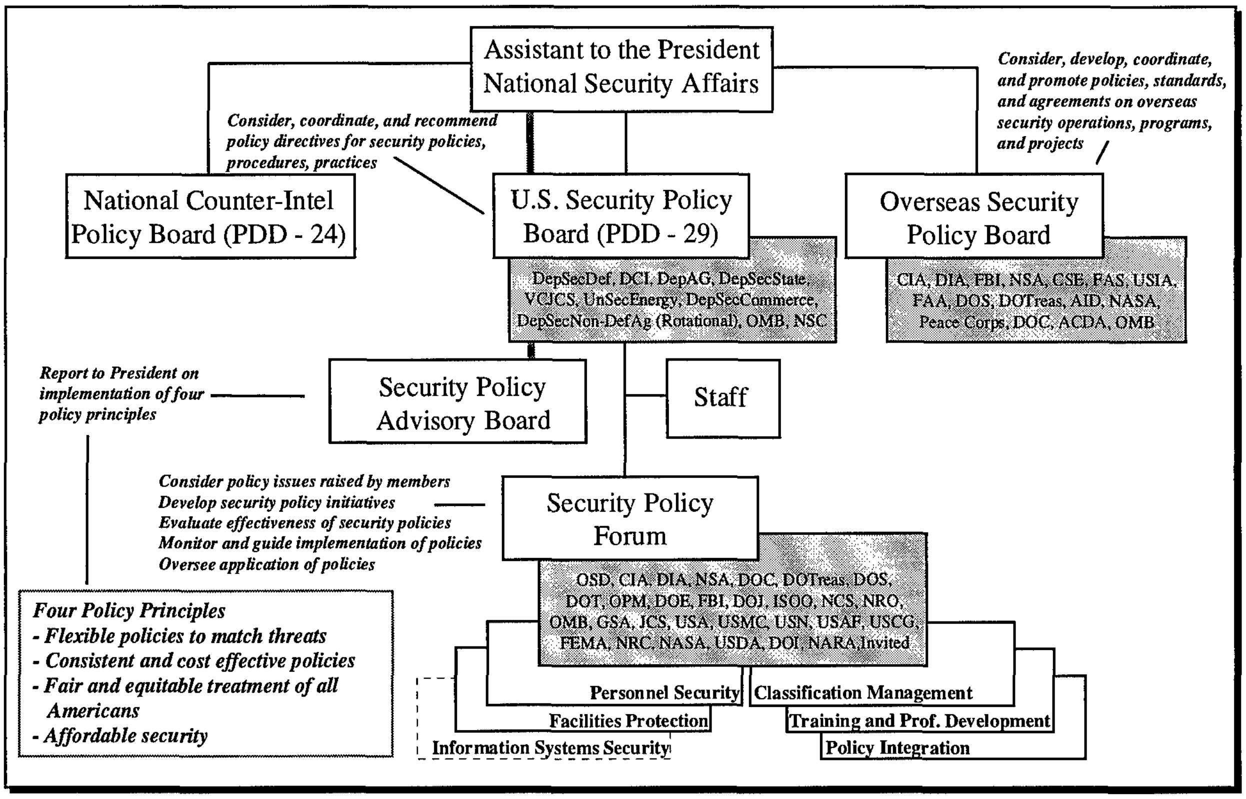

Assistant to the President National Security Affairs
Consider, coordinate, and recommend policy directives for security policies, procedures, practices
Consider, develop, coordinate, and promote policies, standards, and agreements on overseas security operations, programs, and projects
National Counter-Intel Policy Board (PDD - 24)
U.S. Security Policy Board (PDD - 29)
Overseas Security Policy Board
DepSecDef, DCI, DepAG, DepSecState, VCJCS, UnSecEnergy, DepSecCommerce, DepSecNon-DefAg (Rotational), OMB, NSC
CIA, DIA, FBI, NSA, CSE, FAS, USIA, FAA, DOS, DOTreas, AID, NASA, Peace Corps, DOC, ACDA, OMB
Report to President on implementation of four policy principles
Security Policy Advisory Board
Staff
Consider policy issues raised by members
Develop security policy initiatives
Evaluate effectiveness of security policies
Monitor and guide implementation of policies
Oversee application of policies
Security Policy Forum
OSD, CIA, DIA, NSA, DOC, DOTreas, DOS, DOT, OPM, DOE, FBI, DOJ, ISOO, NCS, NRO, OMB, GSA, JCS, USA, USMC, USN, USAF, USCG, FEMA, NRC, NASA, USDA, DOI, NARA,Invited
Four Policy Principles
- Flexible policies to match threats
- Consistent and cost effective policies
- Fair and equitable treatment of all Americans
- Affordable security
Personnel Security
Classification Management
Facilities Protection
Training and Prof. Development
Information Systems Security
Policy Integration

Figure 2-1-7. U.S. Security Policy Board

A second Federal government-level activity is the National Communications System (NCS). The National Communications System is a confederation of the telecommunications assets of 23 Federal departments and agencies. Over 90 networks, such as the Diplomatic Telecommunications Service, FTS 2000, the Defense Switched Network, the Justice Telecommunications Service, and the FEMA Switched Network, make available an extensive array of telecommunications and data services to the NCS member organizations. A few of the specific NCS programs and information assurance activities include:

- GETS. The Government Emergency Telecommunications Service provides National Security/Emergency Preparedness (NS/EP) users with dependable and flexible switched voice and voice-band data communications during times of extreme emergency or war. GETS derives its service from the assets and capabilities of the Public Switched Network (PSN). This emergency telecommunications service is provided by a variety of techniques. One technique restricts access to the priority services to only NS/EP users. Another technique provides priority treatment for GETS calls in the form of priority trunk queuing and reservation, exemption from restrictive management controls (e.g., call blocking) imposed during periods of excessive network loading, and uses a special NS/EP identifier for priority call identification and call set up. Finally, routing of the NS/EP calls through the network is accomplished by an enhanced process which increases the number of possible routes searched—in normal operations, a trunk busy signal is returned to the originator of the call in the event the signaling system makes three unsuccessful attempts to find a route to the call destination.

- TSP. The Telecommunications Service Priority System establishes the regulatory, administrative, and operational framework to authorize the priority provisioning and restoration of NS/EP telecommunications services by the local and long-distance telecommunications carriers. Five levels of priority are provided for the restoration of service and an additional level designated "Emergency" is available for the provisioning of service.

- NTMS. The National Telecommunications Management Structure provides a comprehensive, survivable, and enduring management capability for initiating, coordinating, restoring, and reconstituting the telecommunications resources of the Nation. The Structure includes a cadre of emergency telecommunications managers from both industry and government taking policy direction and guidance from the Director, OSTP. By Executive Order, the Director, OSTP, is assigned responsibility for directing the exercise of the President's wartime authorities over domestic telecommunications which derive from the Communications Act of 1934. In emergencies or crises in which the exercise of the President's war power functions is not required or permitted by law, the OSTP Director is charged with the responsibility to advise and assist the President and Federal departments and agencies with the provision, management, or allocation of telecommunications resources. The structure consists of over 50 industry and government operations centers located throughout the United States. The focal point for these centers is the National Coordinating Center located in the Washington, DC, area and staffed by government and telecommunications industry representatives. The structure is supported by a multimedia National Telecommunications Coordinating Network, which provides communications connectivity for the exchange of minimum essential telecommunications management information.

- GNSIE. The Government Network Security Information Exchange was formed in conjunction with the NSTAC NSIE for the purpose of sharing information on threats, vulnerabilities, and intrusions among government agencies and with industry.

At the national level, two organizations are of interest: the President's National Security Telecommunications Advisory Committee and the Information Infrastructure Task Force.

The NSTAC was created by EO 12382 (see Figure 2-3-4 in Section 2-3) in the aftermath of the divestiture of AT&T and the deregulation of the telecommunications industry. The NSTAC provides the President with advice and information on national security and emergency preparedness telecommunications. Some of its ongoing infrastructure assurance activities include:

- NIITF. The National Information Infrastructure Task Force of the NSTAC is developing the concept and charter for an Information Systems Security Board (ISSB) to serve as a security center of excellence. The goals of the Board will be to adopt security evaluation standards and techniques; coordinate development of security standards; develop and promulgate methodologies for testing and rating security products and services; and educate private, corporate, and organizational users, providers, and decision makers about security issues. It is anticipated that the Board will be based on the Financial Accounting Standards Board model and that it will be a private-sector based, privately funded organization with members coming from the user community, the service provider community, the vendor community, and professional associations.

- NSIE Risk Assessment. The Government and NSTAC Network Security Information Exchanges of the NSTAC recently published their most recent assessment of the risk to the public switched network from electronic intrusion. [NSTAC 1] The report entitled *An Assessment of the Risks to the Security of Public Networks*, December 1995, revealed that the risk is greater than that described in the 1993 report; that deterrent capabilities are increasing, but not fast enough to meet the threats; that protection measures are improving, but not fast enough; that R&D is insufficient; and that there is no nation-wide indications, warning, and assessment capability.

- IATF Risk Assessments. The President has asked the NSTAC to investigate efficient and innovative ways to protect critical information systems and networks. In response, the Information Assurance Task Force of the NSTAC, in conjunction with the Office of the Manager, National Communications System, will conduct risk assessments of the information systems and networks that support three of the nation's critical infrastructures: energy (specifically, power generation, transmission, and distribution), finance, and transportation. The energy assessments began in May, 1996, and should be completed by the end of 1996. It is expected that the other two will be completed by the end of 1997.

- CPAS Assistance. The Federal government is attempting to implement a Cellular Priority Access Service for critical NS/EP users. The NSTAC Wireless Services Task Force has provided advice, assistance in standards development, and implementation support to users and service providers.

One aspect of infrastructure assurance is sharing information about attacks experienced and conducting an open dialog about related security issues. NCS and the NSTAC have established a process that enables telecommunications and information industry members to share sensitive, competitive information regarding threats, vulnerabilities, and intrusions without violating antitrust restrictions. This process, based on extensive non-disclosure agreements and a hierarchy of information sensitivity, also allows government and industry to share similar information. Both the NSTAC and the Federal government formed Network Security Information Exchanges to implement the process. Each NSIE consists of approximately nine member organizations. The NSIEs meet jointly every two months and individually as necessary. For the NSTAC NSIE meetings and the joint meetings, a Designated Federal Official is always in attendance to preclude the possibility of anti-trust issues being raised. Figure 2-1-8 illustrates the entities that were created to facilitate this sharing of information.

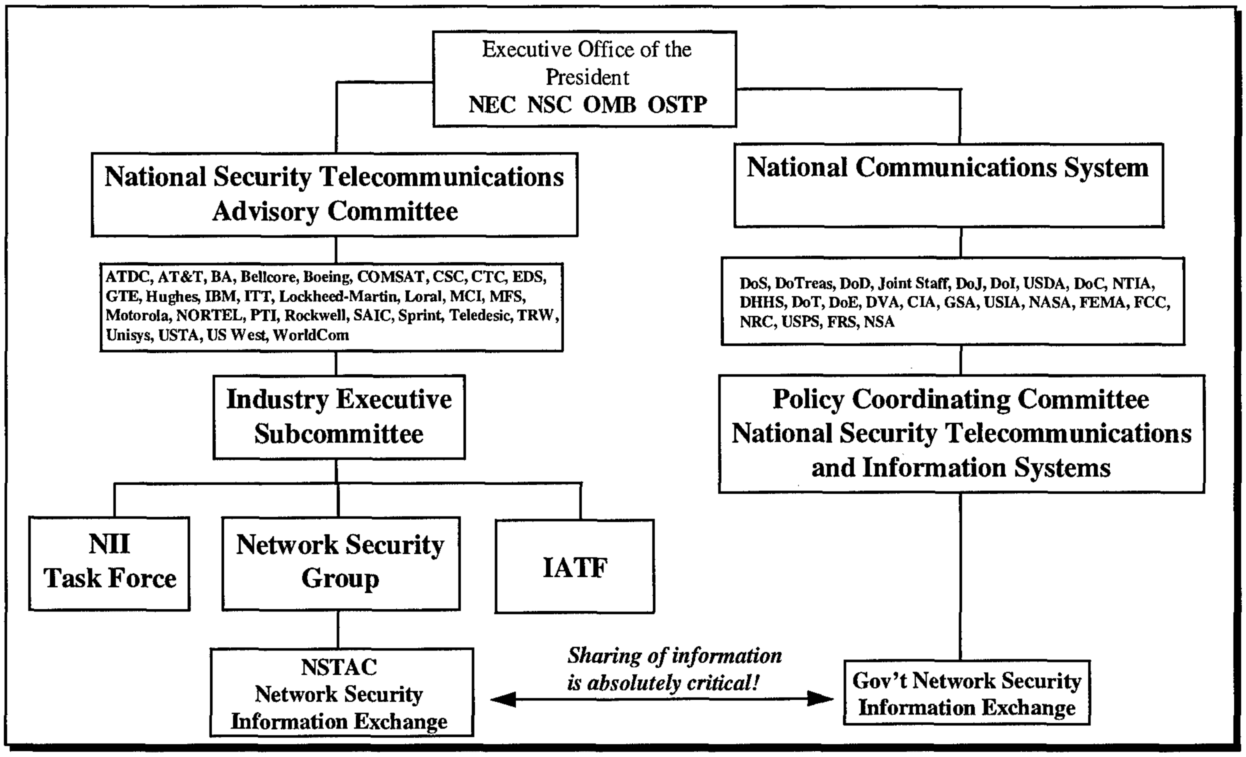

Executive Office of the President
NEC NSC OMB OSTP
National Security Telecommunications Advisory Committee
ATDC, AT&T, BA, Bellcore, Boeing, COMSAT, CSC, CTC, EDS, GTE, Hughes, IBM, ITT, Lockheed-Martin, Loral, MCI, MFS, Motorola, NORTEL, PTI, Rockwell, SAIC, Sprint, Teledesic, TRW, Unisys, USTA, US West, WorldCom
Industry Executive Subcommittee
NII Task Force
Network Security Group
IATF
NSTAC Network Security Information Exchange
National Communications System
DoS, DoTreas, DoD, Joint Staff, DoJ, DoI, USDA, DoC, NTIA, DHHS, DoT, DoE, DVA, CIA, GSA, USIA, NASA, FEMA, FCC, NRC, USPS, FRS, NSA
Policy Coordinating Committee National Security Telecommunications and Information Systems
Gov't Network Security Information Exchange
Sharing of information is absolutely critical!

Figure 2-1-8. NSTAC-NCS Model for Sharing Sensitive Information

Given the market forces at play, it is clear that some form of incentives and indemnification will be required for private industry to share its most sensitive information. [USSPB] It is interesting to note that by the Price-Anderson Act of 1957, the nuclear power industry was granted some limits on liability for nuclear accidents in exchange for regulation and oversight (primarily operational and safety inspections) by the Federal government. [USNRC]

The second national level activity oriented on infrastructure assurance (specifically reliability, security, and privacy) is the Information Infrastructure Task Force (IITF) (shown in Figure 2-1-9), which was created by the President in 1993. (Appendix A contains the details of the task force, its subordinate committees, and its working groups.) Entities specifically dealing with reliability and security issues are the Reliability and Vulnerability Working Group (RVWG), the Government Information Technology Services Working Group, and the Security Issues Forum, which was created because of the number of security issues being raised by the IITF. The Security Issues Forum released its report, *NII Security: The Federal Role* in June, 1995. [OMB] The report is summarized in Appendix B, Policy section. With the exception of the RVWG, these entities have focused on privacy and intellectual property rights issues, not on network reliability and information availability issues.

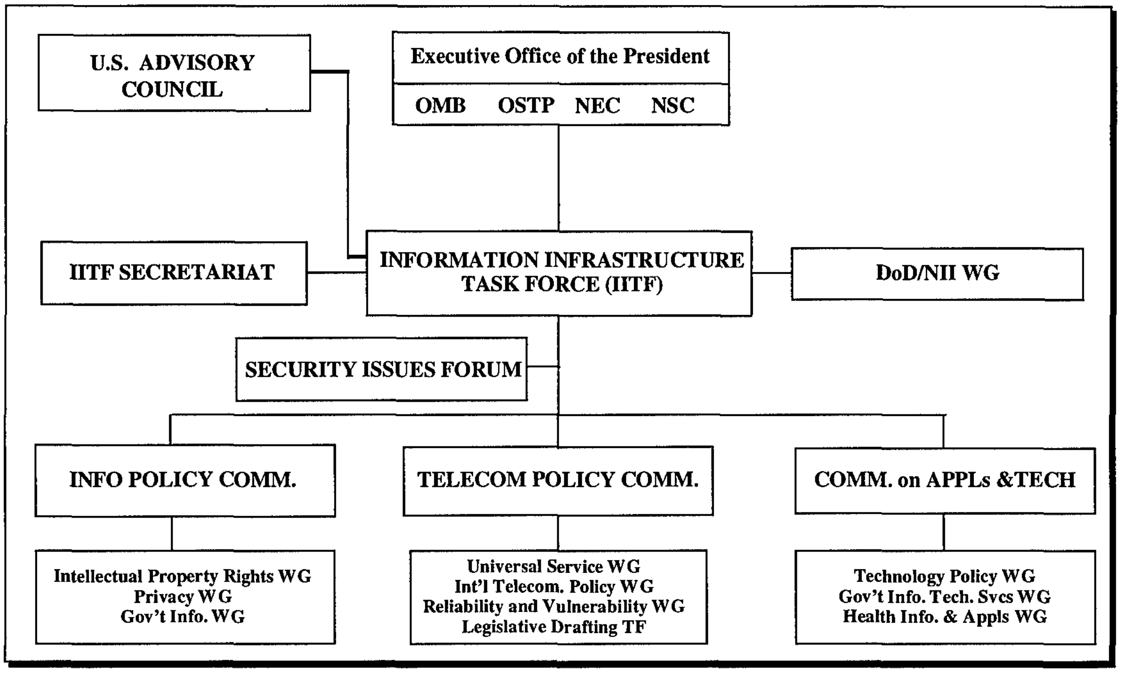


Figure 2-1-9. Information Infrastructure Task Force, Committees and Working Groups

Some recent IITF activities include:

- USAC on the NII. In January 1996, the U.S. Advisory Council on the National Information Infrastructure issued its final report, entitled *A Nation of Opportunity: Realizing the Promise of the Information Superhighway,* and officially disbanded. [USAC] Relevant highlights from the Council's report are extracted below.
  - The United States stands today in the midst of one of the great revolutions in recorded history: the Information Age. The Information Superhighway provides the infrastructure that enables enormous benefits in education, economic well-being, and quality of life.
  - Electronic Commerce. The Federal government, in conjunction with others, should take the steps to identify and resolve, wherever possible, legal, regulatory, and policy issues that would restrict the development of electronic commerce on the Information Superhighway.
  - The Federal government should convene a broad-based committee composed of those entities involved in standard setting, those involved with the development of new technology, and relevant state, local, and tribal agencies to meet the needs of the emergency management, public safety, and criminal justice communities.
  - The Federal government should encourage private sector awareness of security issues, initiate a public-private security consultation process, and foster mechanisms to promote private accountability for proper use of security measures.
  - The Federal government should not inhibit the development and deployment of encryption by the private sector.

- RVWG. The Reliability and Vulnerability Working Group of the Information Infrastructure Task Force Telecommunications Policy Committee has issued a report entitled *NII Risk Assessment: A Nation's Information at Risk.* [RVWG] The report concluded, among other things, that:

  - There are real and active threats to the NII and those threats will grow over time.
  - There is no common framework, approach, or terminology for discussing or analyzing risks to the NII.
  - No sound mechanism exists for government and industry to share information necessary for future sound risk assessments on individual systems.
  - Risk management must be a coordinated effort involving many different activities.
  - Because the NII is so broad and complex, its risk can only be assessed at a high level.

  The emphasis of the report recommendations were centered on the need to establish mechanisms to support information exchange between all NII users detailing how they use the NII, how the risks to the NII will affect them, and what to do to manage those risks.

In spite of these DoD, Federal government, and national-level activities, and other numerous and diverse activities, some key areas have not been addressed. One such area is the significant difference between infrastructure design and system design. System design assumes working components. However, the infrastructure is expected to function in the presence of: failed components, systems, and networks; disruptions in timing; and other disruptive forces. There does not appear to be any ongoing research being devoted to infrastructure design. During crises, the demand for information will increase; the infrastructure capacity will decrease. There is no mechanism in place to determine the priority of information requirements and allocate diminishing infrastructure capacity during such a crisis.

As mentioned earlier, this discussion is not intended to be exhaustive. The references and additional resources contained in Appendix B provide additional insight into these and related issues.

2.2 LEGAL ENVIRONMENT

WHAT'S NEW?

This section has been revised to address new roles and responsibilities and potential effects of the Telecommunications Act of 1996, the Kyl Amendment (National Defense Authorization Act for 1996), the Paperwork Reduction Act of 1995, and the Information Technology Management Reform Act of 1996. Additional information with respect to the Internet and computer crime has also been added.

2.2.1 Introduction

This section reviews portions of the U.S. Constitution and the U.S. Code that are relevant to defensive information warfare. The principal purpose is to identify assigned roles and responsibilities relevant to IW-D and to identify statutes bounding defensive information warfare/information assurance activities. It also discusses the implications of international law and agreements.

It takes years of review and interpretation in precedent-setting cases for public law to become specific. Even so, unique aspects of a case or changes in the environment such as new technology can result in new interpretations of long-standing law. For brevity, little attention is given to case law or to legal issues which do not generally apply to DoD. Except as otherwise noted, references to an Act include the cited Act as amended by subsequent legislation.

The following narrative takes the reader on a legal *walk around the block*, without attempting to interpret the more complex legal issues.

2.2.2 U.S. Constitution

The U.S. Constitution establishes the structure of the U.S. Federal government and delegates the authority of the Federal government to act in particular instances. The Bill of Rights defines certain protected rights. In defining structure and rights, bounds on government activities and broad responsibilities can be interpreted in the context of defensive information warfare.

Bounds. The intent of the Bill of Rights was to guarantee certain rights to citizens and residents of the United States, by restricting the authority the state and Federal government. Several of the amendments are relevant to IW-D. The First Amendment guarantees free speech and limits the authority of the Federal and state governments from restricting the rights of citizens to express themselves. The Fourth Amendment protects citizens from unreasonable governmental searches or seizures and limits the authority of the government to engage in surveillance of U.S. citizens or others who are physically located in the United States or whose property may be located in this country. The Ninth Amendment sets out the principle that individuals (or state governments) retain autonomy, and that any power not delegated to the Federal government is reserved. The Fifth and Fourteenth Amendments establish the proposition that an individual may not be deprived of life, liberty, or property except by "due process of law." According to an Office of Technology Assessment 1994 report, the U.S. Supreme Court has also found privacy implications in other provisions of the Third, Fifth, and Fourteenth Constitutional Amendments [OTA 1]. These amendments are shown in Figure 2-2-1.

AMENDMENT 1 Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances.

AMENDMENT 3 No Soldier shall, in time of peace be quartered in any house, without the consent of the Owner, nor in time of war, but in a manner to be prescribed by law.

AMENDMENT 4 The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

AMENDMENT 5 No person shall be held to answer for a capital, or otherwise infamous crime, unless on a presentment or indictment of a Grand Jury, except in cases arising in the land or naval forces, or in the Militia, when in actual service in time of War or public danger; nor shall any person be subject for the same offence [sic] to be twice put in jeopardy of life or limb; nor shall be compelled in any criminal case to be a witness against himself, nor be deprived of life, liberty, or property, without due process of law; nor shall private property be taken for public use, without just compensation.

AMENDMENT 9 The enumeration in the Constitution, of certain rights, shall not be construed to deny or disparage others retained by the people.

AMENDMENT 14 Section 1. All persons born or naturalized in the United States, and subject to the jurisdiction thereof, are citizens of the United States and of the State wherein they reside. No State shall make or enforce any law which shall abridge the privileges or immunities of citizens of the United States; nor shall any State deprive any person of life, liberty, or property, without due process of law; nor deny to any person within its jurisdiction the equal protection of the laws.

[Amendments 1 through 10 make up the Bill of Rights, ratified on December 15, 1791. Amendment 14 was ratified in 1868.]

Figure 2-2-1. Constitutional Amendments with Privacy Implications

Responsibilities. In addition to ensuring citizens' rights, the Constitution charges Congress with providing for "the common defense and general Welfare of the United States," and the following additional responsibilities which are relevant to information warfare:

- "...securing for limited Times to Authors and Inventors exclusive Right to their respective Writings and Discoveries".
- "To define and punish ... Offences [sic] against the law of Nations".
- "To declare War".
- "To regulate interstate and foreign commerce".

- "To make all Laws which shall be necessary and proper for carrying into Execution the foregoing Powers."

The Constitution provides more general roles and responsibilities to the Executive and Judicial Branches. It vests all executive powers in the President and appoints him the Commander-in-Chief of the Armed Forces. The Judicial Branch, responsible for all cases "arising under this Constitution, the Laws of the United States, and Treaties made" balances the authority of the Legislative and Executive Branches. Moreover, the Judiciary has assumed the role of determining whether acts of Congress and the Executive Branch violate the terms of the Constitution.

Responsibilities constitutionally assigned to the three branches of the Federal government serve to check and balance authority, ensure stability, and prevent the autocracy of a single branch of government or point of view. The Constitution provides the genesis of one of the more controversial issues related to information warfare: the conflict between a citizen's right to privacy—the right to be left alone—and the responsibility of the government to provide for the welfare and common good and ensure economic and national security.

2.2.3 Public Law—U.S. Code

The legislative process is often difficult to follow for those without understanding and access. Legislation originates in the subcommittees and committees of Congress or is proposed by the Administration for consideration by Congress. On significant issues, several bills may be considered and combined. Amendments are frequently offered after a bill reaches the floor of the House or Senate. Joint committees may be formed to resolve differences between bills approved by the two houses of Congress. It is often difficult to monitor the progress of a bill, as it may languish in committee or be quickly passed on the eve of recess or adjournment. On-line resources (information and search engines), such as those provided by the Library of Congress and the House of Representatives, make information on pending legislation and the U.S. Code more readily accessible to the layman. However, a layman may incorrectly interpret pending legislation or the U.S. Code without amplifying information such as committee reports and legislative history or an underlying understanding of associated case law. Also, legislation which does not overtly apply to the DoD may affect the DoD's IW-D activities. It is important, therefore, that Legislative Liaison Officers and General Counsels understand the full scope of IW-D issues and advise policymakers on significant legislative activity.

Each statute of the U.S. Code was drafted, passed, and signed in the hope of achieving certain goals and objectives. Legislation relevant to defensive information warfare can be grouped into four areas. These areas reflect recurring broad objectives envisioned by Congress and the President:

- Protecting Individual Privacy and Providing Access to Government Information.
- Securing Federal Information and Information Systems.
- Ensuring Infrastructure Availability and Reliability.
- Defining the Criminality of Computer Fraud and Abuse.

This section uses these objectives to focus the discussion of the U.S. Code. Several statutes address more than one objective. For example, in an effort to guarantee individual *privacy*, Congress levied *security* requirements on Federal information systems containing personal information. Thus one Act may be discussed in more than one of the following sections. These objectives may also conflict. Computer crime legislation, for example, will normally have privacy implications. The discussion identifies these conflicts as appropriate, particularly those relevant to the DoD.

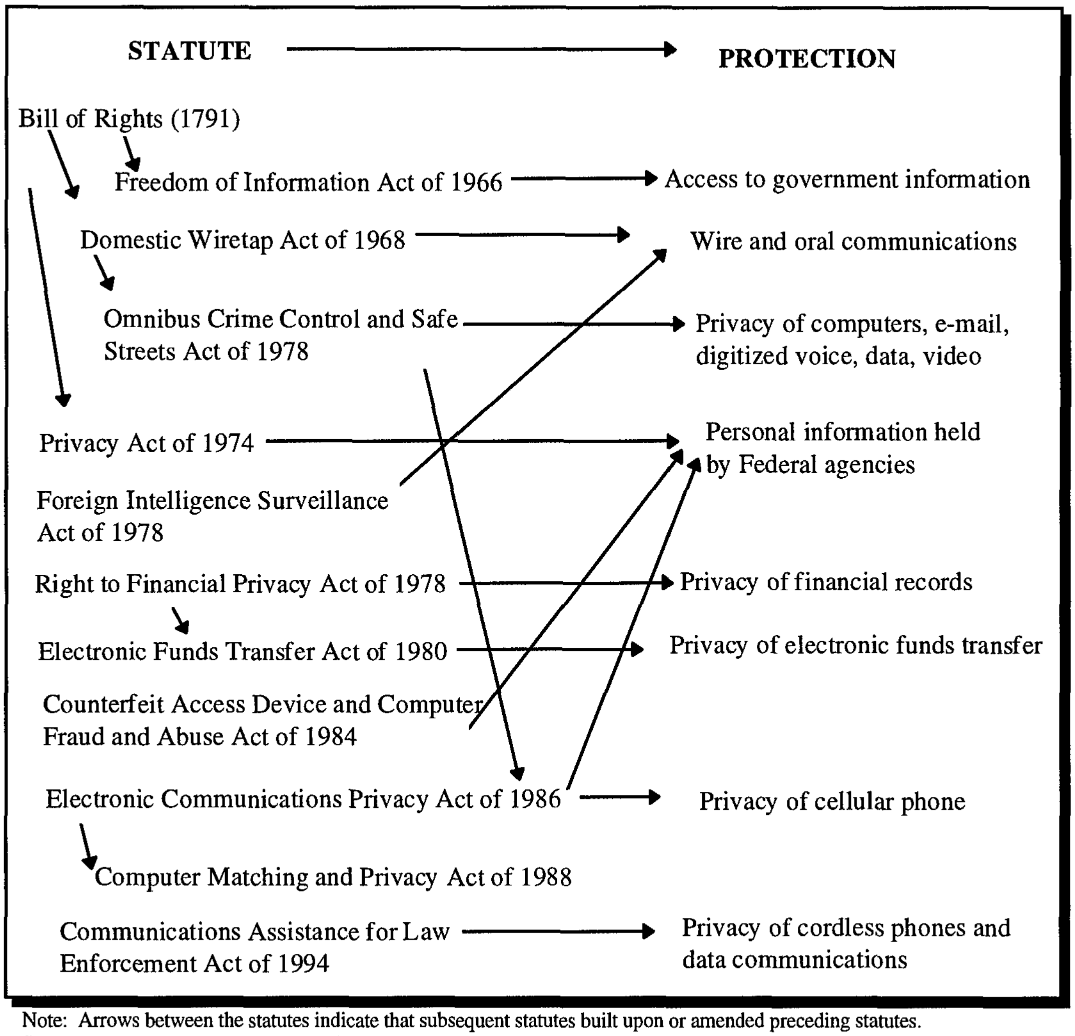
Roles and responsibilities assigned by key statutes are summarized in Figures 2-2-12 through 2-2-20 at the end of the section. Other relevant statutes are summarized in the form of annotated bibliographies in the section entitled U.S. Code in Appendix B, Reference.

2.2.3.1 Protecting Individual Privacy and Providing Access to Government Information

Two aspects of individual privacy are subject to Federal legislation. The first is the protection of individuals' privacy from intrusion by third parties. Examples include protection against collection and dissemination of certain types of personal information (e.g., medical records, financial records, and arrest reports). The second aspect is the protection of individuals' privacy rights from intrusion by the government and governmental agencies (including law enforcement and intelligence agencies). This would include limitation on the government's ability to collect certain types of information (search and seizure and surveillance) and limitations on the ability of the government to disseminate information lawfully collected (e.g., tax information, privacy related information). A final goal of legislation—which often complicates efforts to ensure individual privacy—is ensuring citizens' access to information collected by the government.

Openness of the government—the availability of government information—to its citizens is a recurring theme of legislation (Figure 2-2-2). In 1966, the Freedom of Information Act required that government information, excluding national security, foreign relations, and certain law enforcement information, be made available to citizens. Equally concerned with the potential for abuse created by the massive amount of personal data held by government agencies, Congress passed the Privacy Act of 1974 and subsequent bills to limit the impact of technology on individual privacy and to state explicitly that, while general governmental information is assumed to be public information, information specific to any one individual is protected from disclosure.

The quantity of the legislation depicted in Figure 2-2-2, reflects the extent of Congressional concern for the impact of technology on privacy. Congress sought to ensure the privacy of personal information held by both federal and state governments as well as industries, such as financial and medical, that routinely maintain and transfer personal information.


STATUTE
PROTECTION
Bill of Rights (1791)
Freedom of Information Act of 1966
Access to government information
Domestic Wiretap Act of 1968
Wire and oral communications
Omnibus Crime Control and Safe Streets Act of 1978
Privacy of computers, e-mail, digitized voice, data, video
Privacy Act of 1974
Personal information held by Federal agencies
Foreign Intelligence Surveillance Act of 1978
Right to Financial Privacy Act of 1978
Privacy of financial records
Electronic Funds Transfer Act of 1980
Privacy of electronic funds transfer
Counterfeit Access Device and Computer Fraud and Abuse Act of 1984
Electronic Communications Privacy Act of 1986
Privacy of cellular phone
Computer Matching and Privacy Act of 1988
Communications Assistance for Law Enforcement Act of 1994
Privacy of cordless phones and data communications

Note: Arrows between the statutes indicate that subsequent statutes built upon or amended preceding statutes. Several statutes are indented from the left margin to make these relationships clearer. This indentation does not indicate a subordinate role or lesser effect.

Figure 2-2-2. Privacy and Access to Government Information

The Privacy Act of 1974 arose from Congressional fear that automation was allowing federal agencies to accumulate an increasing amount of personal information. The Act requires the government to ensure reasonable safeguards as technology advances and as information becomes more easily accessible. It is important to note that by focusing on the information rather than the storage medium, the Act requires that federal agency safeguards be as dynamic as the technological environment. Thus, an Act from the *era of mainframes* is equally relevant in the current era of Networks/Internet/Intranets.

Subsequent legislation, the Computer Matching and Privacy Act, restricted Federal use and disclosure of information resulting from computer matching capabilities. *Computer matching* compares information from different data bases to detect fraud, waste, and abuse; principally in benefit programs. As electronic fund transfers became commonplace, Congress required the financial community to ensure privacy equivalent to that provided when funds and financial information were transferred by mail or courier.

As technology advanced, Congress found itself defining new methods of exchanging information in which a citizen had a legitimate expectation of privacy. Protection was initially extended to wire and oral communications in 1968 by the Domestic Wiretap Act. Subsequent amendments added computers, electronic mail (e-mail), and cellular phones to the list in 1986; cordless phones were added in 1994. Various types of data communications were defined and added by succeeding statutes. Today, unauthorized interception is illegal for almost every type of electronic or wire communication regardless of the type of information (e.g., voice, data, or video) or medium (e.g., cordless, cellular, or fiber optic) except for radio communications readily accessible to the general public. Any encrypted or scrambled information, even using transmission techniques such as spread spectrum, are not considered readily accessible and therefore, unauthorized interception is illegal. The lack of privacy on the Internet is well documented and Congress has not codified an expectation of privacy on the Internet or to users of Internet e-mail. Like its predecessors, the 104th Congress has shown continued interest in the impact on individual privacy resulting from new technological capabilities. House and Senate resolutions were offered requiring government agencies and others (such as health providers and on-line service providers) to ensure the privacy of customer information and to refrain from resale of consumer information. The Paperwork Reduction Act of 1995 (Public Law 104-13) reiterates the Federal government responsibility, under Office of Management and Budget (OMB) supervision, to protect sensitive information in accordance with existing statutes, such as the Computer Security Act of 1987.

Congress has also established processes to ensure the primacy of the privacy of U.S. citizens and residents in clandestine electronic intelligence gathering activities. The Foreign Intelligence Surveillance Act of 1978 established a process to facilitate electronic acquisition of foreign intelligence within the United States while minimizing the impact on U.S. residents. Court orders (commonly referred to as Title III orders by the law enforcement community) are required unless the Attorney General, on behalf of the President, certifies in writing the purposes and procedures to be employed to minimize the impact on U.S. residents. Several other acts and Executive Orders assign intelligence gathering responsibilities, including oversight and jurisdiction. The Central Intelligence Agency (CIA) and the Federal Bureau of Investigation (FBI) have purview over certain types of clandestine operations during peacetime. The FBI is responsible for foreign counter-intelligence operations (investigating foreign agents and U.S. citizens for evidence of prohibited espionage activities) within the United States, while the CIA is the proponent for activities outside the United States. Foreign or domestic covert intelligence activities—which may include clandestine electronic intelligence gathering—require a Presidential intelligence finding (and in certain cases, notification of the appropriate Congressional committees) and must be coordinated with the CIA or the FBI. No agency except the CIA can conduct any special activities without a Presidential determination. As an exception, the Armed Forces may engage in special activities in time of war as declared by Congress or after the President has reported to Congress in accordance with the War Powers Resolution Act.

Figure 2-2-3 depicts a hierarchical chain of responsibility for ensuring individual privacy and citizen access to government information. The Department of Justice (DoJ) (including the

Attorney General and the FBI) and the CIA are charged with minimizing the impact of intelligence and law enforcement activities on citizens. The Privacy Protection Study Commission has a charter encompassing federal, state, and local agencies. OMB publishes privacy guidelines and regulations for the Federal government. The Paperwork Reduction Act of 1980 also assigns OMB responsibility for establishing government-wide information technology management policy. The Paperwork Reduction Act of 1995 assigns OMB specific responsibility for security of federal information systems. These complementing responsibilities make OMB a significant player in the Federal government's information assurance activities.

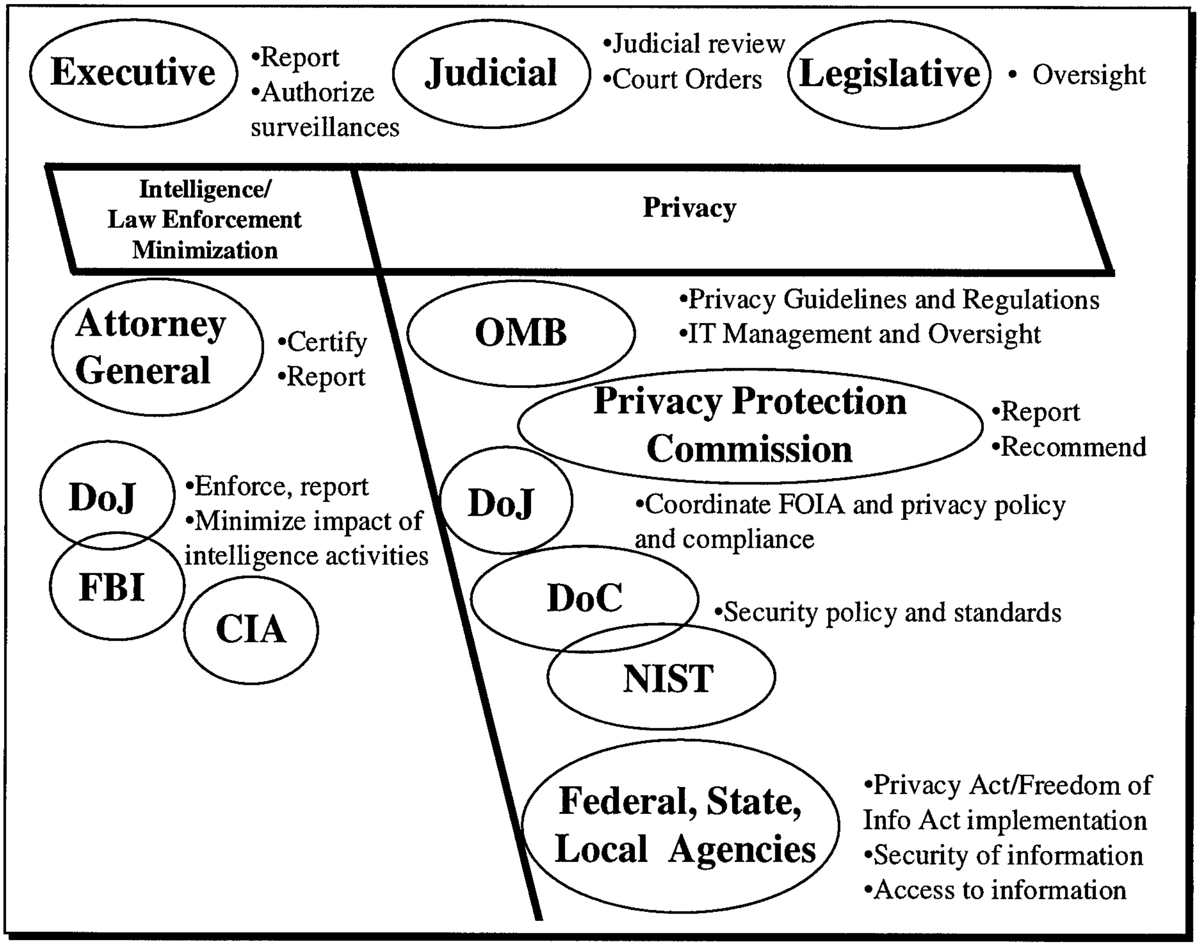

Executive
•Report
•Authorize surveillances
Judicial
•Judicial review
•Court Orders
Legislative
• Oversight
Intelligence/ Law Enforcement Minimization
Privacy
Attorney General
•Certify
•Report
DoJ
FBI
CIA
•Enforce, report
•Minimize impact of intelligence activities
OMB
•Privacy Guidelines and Regulations
•IT Management and Oversight
Privacy Protection Commission
•Report
•Recommend
DoJ
•Coordinate FOIA and privacy policy and compliance
DoC
NIST
•Security policy and standards
Federal, State, Local Agencies
•Privacy Act/Freedom of Info Act implementation
•Security of information
•Access to information

Figure 2-2-3. Government Responsibility for Ensuring Privacy

2.2.3.2 Securing Federal Information and Information Systems

A second objective of legislation is that of securing Federal information and information systems. Categories of information are key to this discussion. Statutes in support of this objective generally address information that is classified for reasons of national security or foreign policy, or information that is sensitive but unclassified. Information or systems that are Warner Exempt are normally included with the classified information. These are systems that are exempt from the provisions of the Brooks Act of 1965 (The Brooks Act was revoked in 1996; see Information

Technology Management Reform Act of 1996 under U.S. Code in Appendix B) by the Warner Amendment because they involve command, control, communications, and intelligence (C3I), cryptography, or electronics embedded in weapons systems or equipment critical to a military or intelligence mission. However, policy documents often apply to the integrity and availability of all Federal information and information systems, regardless of classification or sensitivity.

This section focuses on those government organizations that have statutory responsibility for ensuring the security of Federal government information and information systems.

To assign security responsibilities, statutes have expanded roles assigned in preceding statutes. The Communications Act of 1934 gives OMB and the Department of Commerce (DoC) roles in executive branch telecommunications. The Federal Property and Administrative Services Act of 1949, the Brooks Act of 1965, and the Paperwork Reduction Act of 1980 give OMB, DoC, National Institute of Standards and Technology (NIST), and GSA roles in procuring and managing federal information technology. Because of the roles and efforts already under way in these agencies, the Computer Security Act of 1987 assigned responsibility for security standards and guidelines to DoC, NIST, NSA, and GSA for sensitive unclassified information. This act also established the Computer System Security and Privacy Advisory Board (CSSPAB). Executive Order 12356 subsequently established the Information Security Oversight Office (ISOO) under GSA to oversee compliance with national security information guidance. The ISOO was transferred to OMB by Executive Order 12958.

The Paperwork Reduction Act of 1995 specified a security role for OMB, making the Director responsible for policies, principals, standards, guidelines, oversight and compliance with the Computer Security Act of 1987. It also directs OMB to require Federal agencies to apply a risk management process for information collected or maintained by or on behalf of an agency (Figure 2-2-4).

The Information Technology Management Reform Act, a subordinate act of the National Defense Authorization Act of 1996, repealed the Brook Act which granted oversight responsibilities to GSA for government information technology procurement (see Appendix B, U.S. Code). The new Act requires agencies, under OMB's oversight, to use a performance- and results-based management process for IT acquisitions. The Act also requires agencies to appoint a Chief Information Officer (CIO) responsible for IT acquisition and management. This further consolidates OMB's already key role in government information technology. Also, as CIO responsibilities are further defined, the CIO may serve as an agency central point for information assurance. The OMB is coordinating an executive order to implement the Act.

Figure 2-2-4 portrays the applicable statutes, relationships, and assigned responsibilities. Parentheses indicate organizations with roles assigned by executive direction rather than statutory authority. Figure 2-2-5 provides a hierarchical view of assigned responsibilities for Federal INFOSEC.

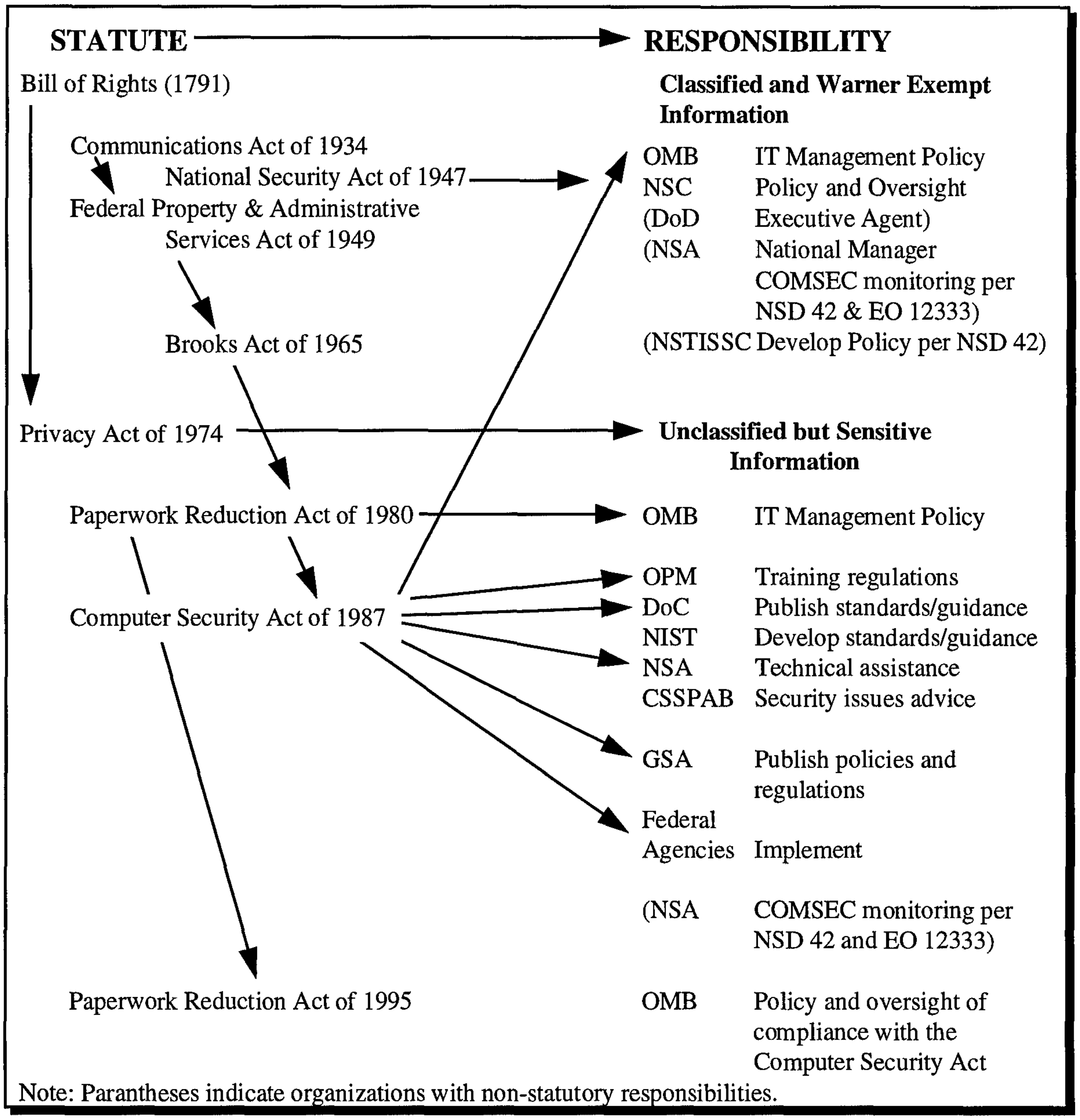

STATUTE
RESPONSIBILITY
Bill of Rights (1791)
Communications Act of 1934
National Security Act of 1947
Federal Property & Administrative Services Act of 1949
Brooks Act of 1965
Privacy Act of 1974
Paperwork Reduction Act of 1980
Computer Security Act of 1987
Paperwork Reduction Act of 1995
Classified and Warner Exempt Information
OMB IT Management Policy
NSC Policy and Oversight
(DoD Executive Agent)
(NSA National Manager COMSEC monitoring per NSD 42 & EO 12333)
(NSTISSC Develop Policy per NSD 42)
Unclassified but Sensitive Information
OMB IT Management Policy
OPM Training regulations
DoC Publish standards/guidance
NIST Develop standards/guidance
NSA Technical assistance
CSSPAB Security issues advice
GSA Publish policies and regulations
Federal Agencies Implement
(NSA COMSEC monitoring per NSD 42 and EO 12333)
OMB Policy and oversight of compliance with the Computer Security Act
Note: Parantheses indicate organizations with non-statutory responsibilities.

Figure 2-2-4. Security of Federal Information Systems

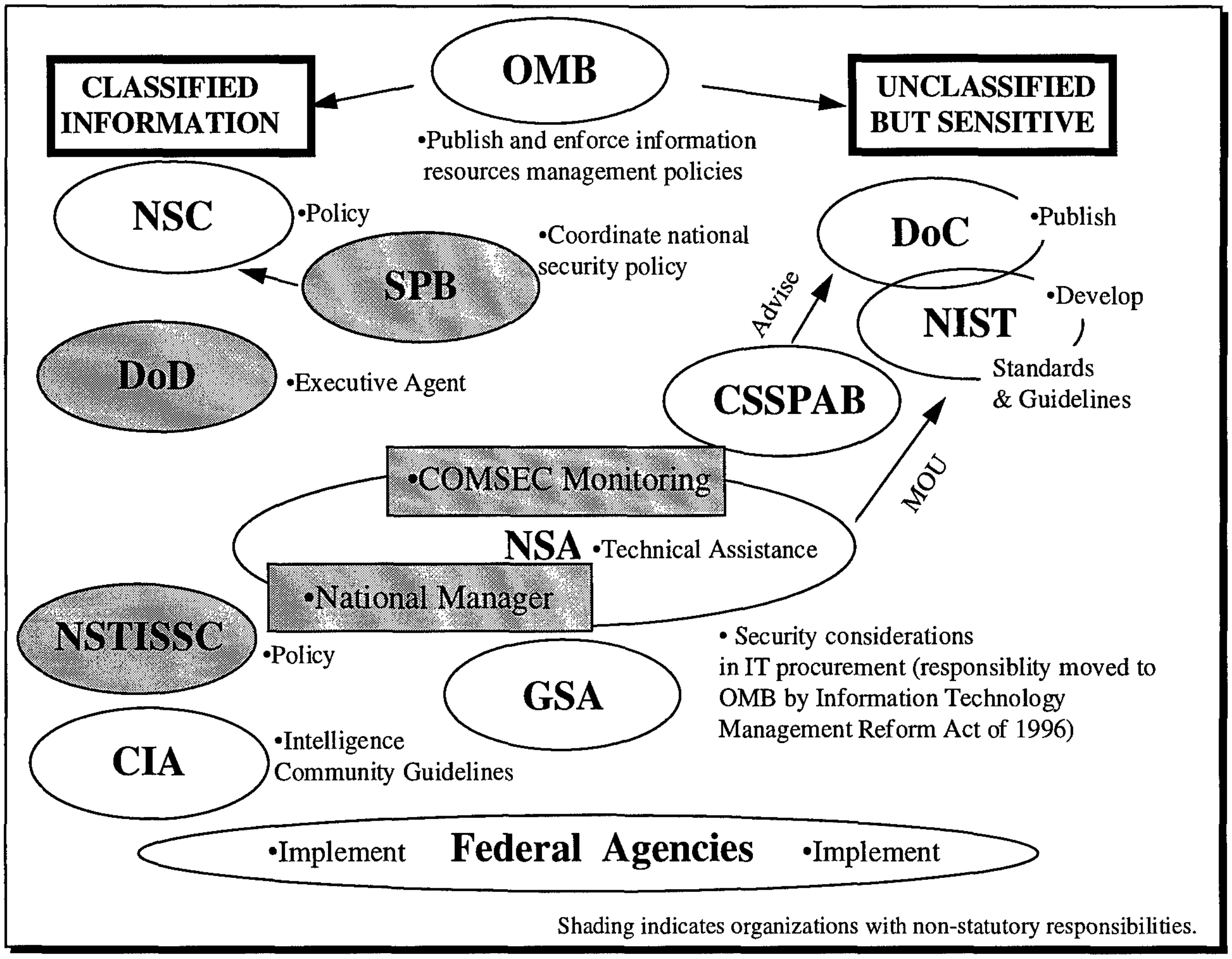

OMB
CLASSIFIED INFORMATION
UNCLASSIFIED BUT SENSITIVE
•Publish and enforce information resources management policies
NSC
•Policy
SPB
•Coordinate national security policy
DoC
•Publish
NIST
•Develop
Standards & Guidelines
Advise
DoD
•Executive Agent
CSSPAB
•COMSEC Monitoring
NSA
•Technical Assistance
MOU
•National Manager
NSTISSC
•Policy
GSA
• Security considerations in IT procurement (responsiblity moved to OMB by Information Technology Management Reform Act of 1996)
CIA
•Intelligence Community Guidelines
•Implement
Federal Agencies
•Implement
Shading indicates organizations with non-statutory responsibilities.

Figure 2-2-5. Responsibility for Information Systems Security

In summary, OMB has a prominent position within the Federal government for all information technology policy and management, and significant roles in budget, privacy, and security. OMB thus plays a key role in information assurance. The NSC plays a similar key role for national security information. Forums in which both participate are key to future information and information system security policy. Policymakers interested in influencing the direction of information policy should monitor and participate in these forums.

An understanding of the background of the Computer Security Act of 1987 is important to understanding sensitivities that remain today. In 1984, President Reagan signed National Security Decision Directive 145 (NSDD 145), National Policy On Telecommunications and Automated Information Systems Security. NSDD 145 appointed the Secretary of Defense the Executive Agent and the Director of NSA the National Manager for national telecommunications and information systems security. These roles made DoD responsible for sensitive but unclassified information as well as classified information. NSDD 145 encouraged the National Manager and Executive Agent to coordinate with the private sector on information systems security. Civil agencies and the private sector expressed concern that NSDD 145 gave the military and intelligence communities too much authority for non-national security information. Subsequent Administration actions, citing NSDD 145 as authority, heightened these concerns. In direct response to this trend, Congress passed the Computer Security Act of 1987, giving primary responsibility for sensitive but unclassified standards and guidelines to the civil side of the Federal government. President Bush signed National Security Directive 42 (NSD 42) in 1990 to bring Executive Branch policy in line with the act.

In 1989, NSA and NIST executed a Memorandum of Understanding (MOU) to clarify roles and responsibilities under the Act. The MOU is not without controversy; some feel the MOU grants NSA greater responsibility for sensitive but unclassified information than provided for in the Act. Civil and private concern with centralizing policy development for classified and unclassified information under a single authority, particularly under the defense/intelligence community, is still prevalent. An example of this concern can be seen in the organizational summary of the U.S. Security Policy Board, provided in Appendix A.

2.2.3.3 Ensuring Infrastructure Availability and Reliability

Early in the 20th century, the Federal government realized that reliability and availability of the telecommunications infrastructure were critical to national security and economic progress. In 1909, Congress passed a law, codified at Title 18, United States Code, Section 1362, which made it a crime to injure or destroy or interfere with any means of communication owned by the United States or used for military or civil defense functions of the United States. The following discussion addresses continuing infrastructure assurance efforts. For the purposes of the discussion, *infrastructure* is not limited to government owned or leased telecommunications infrastructure, but includes the national public infrastructure as well.

The Communications Act of 1934 is the cornerstone to infrastructure reliability and availability. It created the Federal Communications Commission (FCC) to regulate the telecommunications and broadcast industries in the public interest and addressed willful or malicious interference with radio transmissions. The statute also delineated certain key war powers of the President in the area of telecommunications, including the authority to require common carriers to give priority to national defense communications and the authority to employ the armed forces to prevent obstruction of interstate or foreign communications. Figure 2-2-12 lists other Presidential and Executive Branch responsibilities under the Communications Act of 1934.

On February 8, 1996, the President signed the Telecommunications Act of 1996 (Figure 2-2-20). This Act is the most comprehensive revision of the Communications Act of 1934 since it was passed. The principal objective of the Act is to open up local and long-distance telephone service, telecommunications equipment manufacturing, cable television, and radio and television broadcasting to increased competition. A subset of the Act, called the Communications Decency Act of 1996, criminalizes the transmission of indecent material to minors over the Internet and the transmission of annoying or harassing material. It requires television manufacturers to install V-chips in new sets that allow users to block violent or sexually explicit programs. (The U.S. Court of Appeals ruled the Communications Decency Act unconstitutional and granted an injunction preventing prosecution under the law pending appeal. The DoJ has decided to appeal the decision.)

The long-term impact of the Act on the availability and reliability of the Public Switched Network is difficult to determine as many of the details of implementation have been left to the FCC. "The Act requires between 50 to 80 rulemakings by the FCC." [DISA 2]

The DoD Regulatory Counsel-Telecommunications has identified several potential national security issues. One key concern is the potential effect of the new players on the management of NS/EP Programs such as TSP and GETS. Another is the elimination of the requirement for a single point of contact. Under the AT&T Consent Decree, BELLCORE served as the single point of contact for the Bell Operating Companies for NS/EP issues. Although the NCS and RBOC have agreed to maintain BELLCORE as the single POC, this agreement may not carry the same weight as a court order. The Act allows limited foreign ownership of some U.S. telecommunications companies; this, too, engenders national security concerns. While the FCC is charged with developing rules for interconnection and access, the Act contains language that allows interconnection "at any point which is technically feasible." [DISA 2] Some are concerned that implementation of "technically feasible" solutions may adversely affect network security.

Telecommunications Act of 1996
NS/EP Concerns

- New Players may affect NS/EP Programs such as GETS and TSP
- No court ordered single point of contact for NS/EP
- Foreign ownership of telecommunications companies
- Interconnection of new carriers with existing carriers may adversely affect network security
- Applicability of War Powers on new Common Carriers

Figure 2-2-6. NS/EP Concerns with the Telecommunications Act of 1996

The Act did not change Section 706, Presidential War Powers, of the Communications Act of 1934. However, existing war powers apply to PSN Common Carriers. Determining which service providers meet the definition of a Common Carrier is more complex in the competitive environment created by the Act. Section 706 provides the President with certain war powers listed in Figure 2-2-12 with respect to the PSN and radio broadcasting facilities. This section also provides the underpinning for national security and emergency preparedness telecommunications activities. The lack of change to this section can be viewed as favorable because existing powers and activities to enhance PSN reliability and availability may continue unimpeded. However, the powers in this section may need to be reviewed in light of the DoD's increasing dependency on public infrastructures.

The Kyl Amendment (Figure 2-2-19) reflects congressional concern with the potential damage of a strategic attack on critical infrastructures. This amendment asks the President to review national policy and architecture governing the plans for establishing procedures, capabilities, systems, and processes necessary to perform indications and warning functions, and assessment of strategic attacks by foreign nations, groups, or individuals, or any other entity against the national information infrastructure. The Administration is addressing this concern with several initiatives as this report goes to press. Several of these initiatives are discussed in Section 2.1.8, Information Infrastructure Assurance. Figure 2-2-7 shows the continuing Congressional interest in these issues.

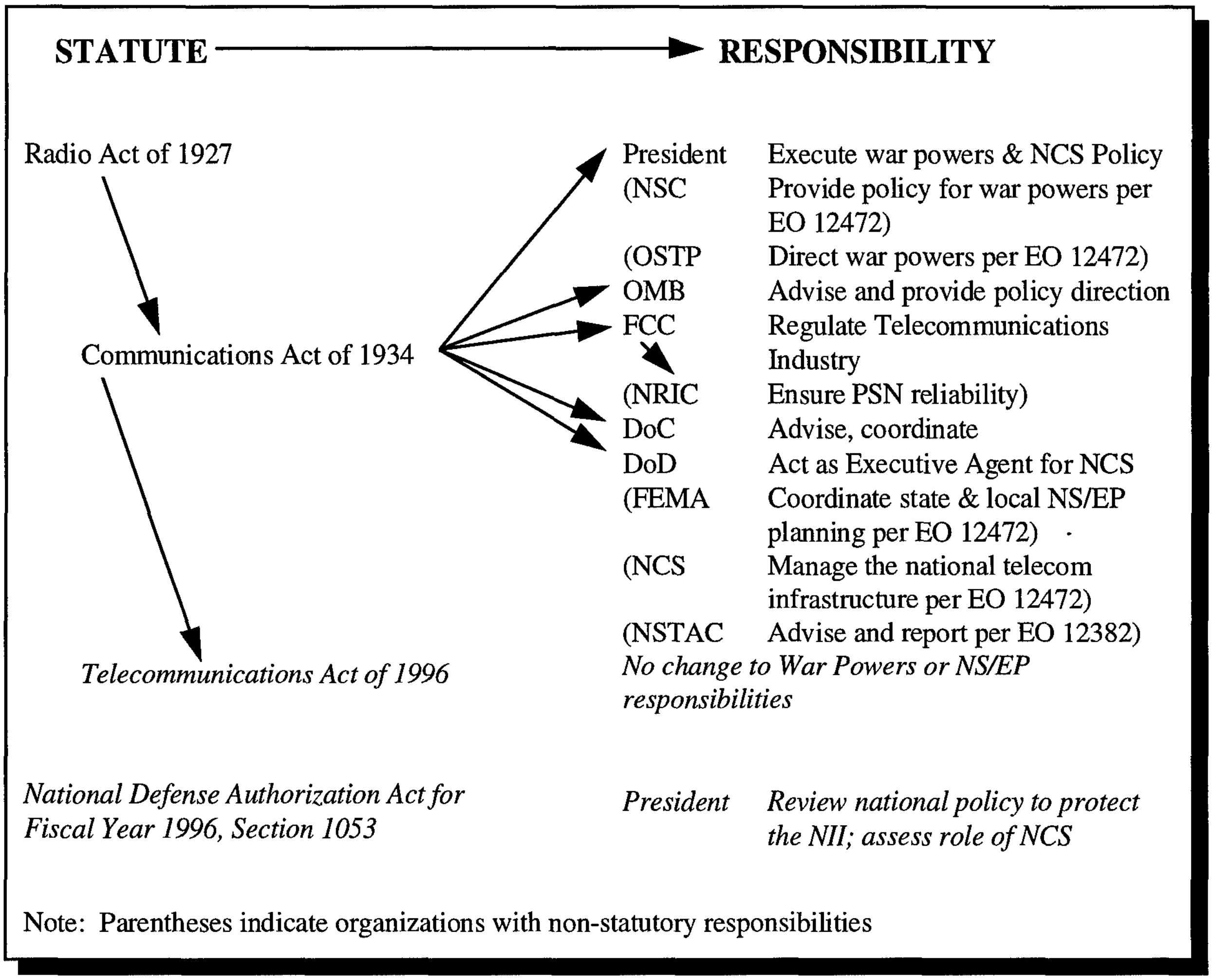
Continuing Congressional Interest in the Protection of the NII
House Resolution 3230

The recently passed House version of the National Defense Authorization Act for Fiscal Year 1997 includes language which:

- Requires the President to report to Congress(as the Kyl Amendment did) "setting forth the national policy on protecting the national information infrastructure against strategic attacks. The report will include:
  - National policy and plans to meet essential Government and civilian needs during a national security emergency associated with an attack on the NII "the functioning of which depend on networked computer systems."
  - Identification of critical functions that must be performed during an emergency
  - Assignment of Federal responsibilities
- Requires the DoD to allocate funds to a separate program element for information security an amount equal to specified percentages f funds allocated to the DII.
  - The percentage increases from 2.5 to 4.0 percent from 1998 through 2001.
  - This funding is to be exclusive of NSA and DARPA funding for INFOSEC.

Figure 2-2-7. House Resolution 3230

Figure 2-2-8 portrays the applicable statutes, relationships, and responsibilities for infrastructure availability and reliability (assurance) arising from the Radio Act and the Communications Act. Parentheses indicate organizations with roles assigned by the President rather than by statute.



STATUTE → RESPONSIBILITY

Radio Act of 1927

Communications Act of 1934

Telecommunications Act of 1996

President	Execute war powers & NCS Policy
(NSC	Provide policy for war powers per EO 12472)
(OSTP	Direct war powers per EO 12472)
OMB	Advise and provide policy direction
FCC	Regulate Telecommunications Industry
(NRIC	Ensure PSN reliability)
DoC	Advise, coordinate
DoD	Act as Executive Agent for NCS
(FEMA	Coordinate state & local NS/EP planning per EO 12472)
(NCS	Manage the national telecom infrastructure per EO 12472)
(NSTAC	Advise and report per EO 12382)

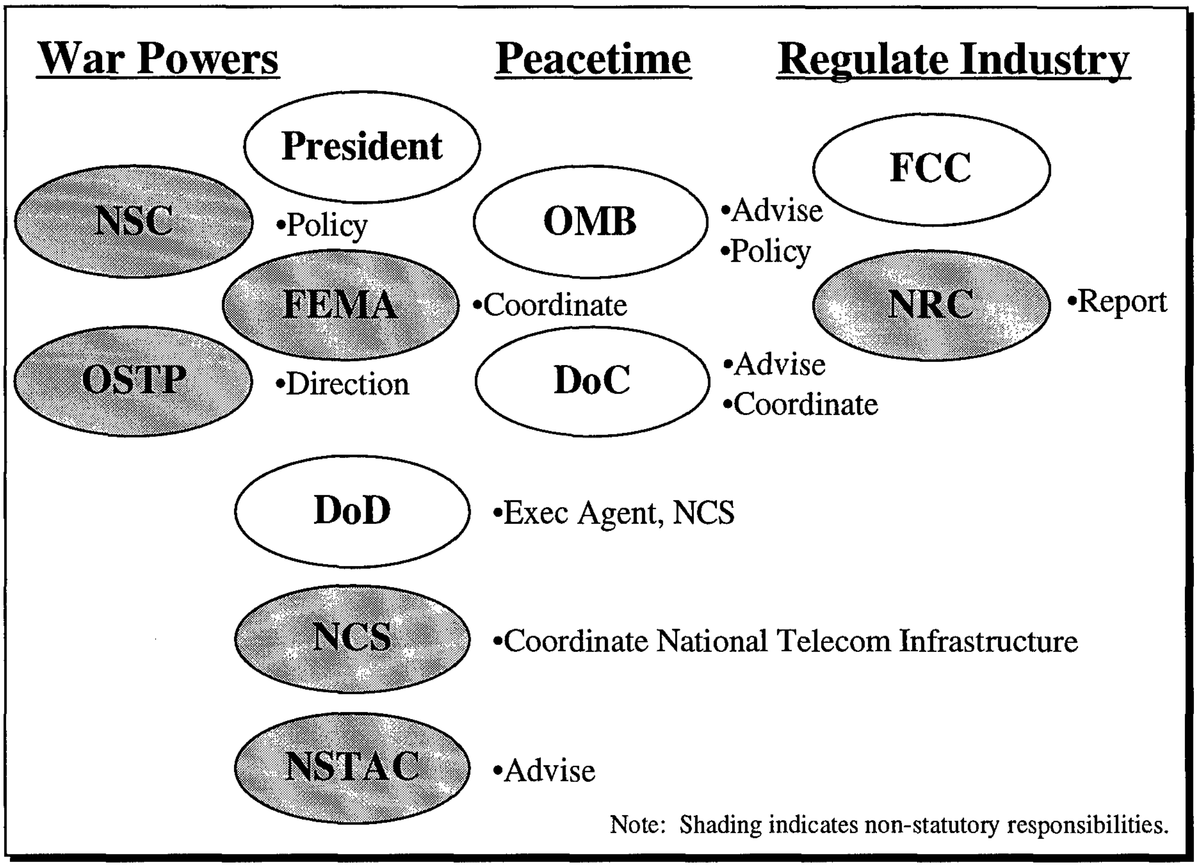
No change to War Powers or NS/EP responsibilities

National Defense Authorization Act for Fiscal Year 1996, Section 1053	*President*	*Review national policy to protect the NII; assess role of NCS*

Note: Parentheses indicate organizations with non-statutory responsibilities

Figure 2-2-8. Infrastructure Availability and Reliability

Figure 2-2-9 portrays a hierarchical chain of responsibility for infrastructure availability and reliability. NSC, OSTP, OMB, and DoC are assigned responsibilities during either war or peace. The President, FEMA, and others have roles during both war and peace.



Note: Shading indicates non-statutory responsibilities.

Figure 2-2-9. Responsibility for Infrastructure Availability and Reliability

2.2.3.4 Defining the Criminality of Computer Fraud and Abuse

The same skills and techniques can be used in both computer crime and information warfare. While there is still much debate over the nature of an act of war in the Information Age, there is general agreement that computer crime must be better defined.

Computer crime has evolved along with technology and automation. So also have the legal views of computer crime. Initially, only crimes in which computers were used as tools were prosecuted. Embezzlement, for example, is a criminal act; therefore, embezzlement using computers was also a crime. However, trespassing into a computer, or examining computer generated files or data (without depriving the owner of these files or their use) was not considered a criminal act. Similarly, simply using a computer without the authorization of the owner was not considered a crime as long as the owner's use of the computer was not significantly affected. Finally, while paper documents could be stolen, the theft of computerized files and data presented difficult legal and burdens of proof problems.

As computer technology became more prevalent and better understood, views as to the criminality of computer fraud and abuse evolved. The Congress passed the Counterfeit Access Device and Computer Fraud and Abuse Act of 1984, the first Federal computer crime legislation.

This statute was significantly overhauled in the Computer Fraud and Abuse Act (CFAA) of 1986. By this time, most states had enacted legislation making theft of computer resources a criminal act. Even with statutes in place, however, computer crimes were often prosecuted as petty larceny, as the value of the stolen or damaged information did not translate easily into terms understood by judge or jury. It is now more commonplace for the value of the information to be considered and judgments rendered accordingly.

The CFAA amended Title 18, United States Code, Section 1030, to enhance penalties for intentional access into Federal Interest Computers for the purpose of committing certain types of criminal conduct. *Federal Interest Computer,* as used in the CFAA, includes computers owned by or used by a financial institution or the Federal government in addition to a computer "which is one of two or more computers used in committing the offense, not all of which are located in the same State." Thus, *any* computer used in interstate or international commerce in the commission of the offense would be covered by this provision. The statute criminalizes six computer activities: (1) the unauthorized access of a computer to obtain information of national secrecy with an intent to injure the United States or advantage a foreign nation; (2) the unauthorized access of a computer to obtain protected financial information; (3) the unauthorized access of a computer intended for the exclusive use of the Federal government; (4) the unauthorized interstate access of a computer system with an intent to defraud; (5) the unauthorized interstate or foreign access of computer systems that results in at least $1000 aggregate damage; and (6) the fraudulent trafficking in computer passwords affecting interstate commerce.

Each of these provisions requires proof that the defendant accessed the computer without authorization. By focusing on the method of *entry* into the computer or computer system, rather than the method of *use* of the computer system, the statute excludes broad categories of potentially criminal conduct. Theft of information by corporate or government insiders, or those with an arguable right to access the computer, could not be punished under this provision. Nor could those who, with authorization to access or use a computer or computer system, alter, damage, or destroy information contained on that system. Similarly, the prosecution of authors or distributors of computer viruses or other forms of malicious code is complicated by the requirement that the government demonstrate the wrongdoer (1) actually accessed the computer; and (2) lacked the authority (explicit or implicit) to do so.

Curiously, the fraud provision of the CFAA expressly prohibits prosecution for the unauthorized access of a computer system where "the object of the fraud and the thing obtained consists only of the use of the computer." Thus, as under the wire fraud statute, the mere viewing of data without authorization may not be criminal under the CFAA. Furthermore, the protection afforded by the CFAA to national secrets, financial records, and government computers does not require an explicit computer crime statute; protection probably exists irrespective of the provisions of the CFAA. The anti-password provision of the CFAA is the most original section of the statute, but to date, there has not been a prosecution under this provision.

Perhaps the most famous application of this statute was the 1989 prosecution of Robert Tappan Morris, a Cornell University graduate student who, on November 2, 1988, released a computer worm across the Internet. The program, designed to surreptitiously spread across the network to thousands of connected computers, inadvertently replicated faster than the defendant intended, and, instead of inserting a copy or two into these networked computers, inserted thousands of copies of the program until the network actually shut down. On appeal, the second circuit court rejected the defendant's arguments that, because he was permitted to send mail to users of computers on the network, he was therefore authorized to access these computers, and further rejected arguments the statute required proof he intended to cause damage to the computers—as distinct from intent to obtain unauthorized access.

Despite the successful prosecution in *Morris*, the predicted explosion of computer crime prosecutions has not occurred. The lack of prosecutions can be attributed to the fact that many computer crimes are committed by insiders with access to the affected computers. In addition, corporations—especially institutions that depend upon public trust and confidence—are reluctant to report computer crimes, which might rode the public's faith. Moreover, there is a perception that computer offenders who cause no quantifiable loss to their victims, but nonetheless obtain confidential information about individuals or organizations, may evade effective punishment under the current Federal sentencing scheme.

Jurisdiction in computer crime presents challenges as it transcends both state and national boundaries. In general, if an offense is wholly conducted within one state, the offense is a state crime. As Table 2-2-1 illustrates, virtually every state prohibits in some fashion the unauthorized access or use of computers. If the offense crosses state lines, or if the victim of the offense is the Federal government, the offense is Federal. If the offense occurs internationally, it may constitute a crime in the country where the offender is located, where the victim is located, or in some instances, in the nation through which the communications travel. These definitions are not mutually exclusive, and an offense may violate local, state, Federal, national and international law simultaneously. Even if the conduct violates the statutes contained within a jurisdiction, a sovereign still must obtain personal jurisdiction over the defendant—that is, the sovereign must extradite the offender. In the United States, the Federal government has nationwide jurisdiction, which may extend to the special maritime jurisdiction (U.S. territorial waters). However, to obtain jurisdiction abroad, the foreign country in possession of the accused must agree to turn the offender over to the United States—usually through extradition. Some countries do not prohibit unauthorized access of foreign systems, and most countries will not extradite unless the offense charged is a crime in that jurisdiction. Most nations are also reluctant to extradite their own nationals.

Table 2-2-1. State Computer Crime Statutes

- ALA. CODE §§ 13A-8-100 to 13A-8-103 (Supp. 1992)
- ALASKA STAT. § 11.46.740 (1989)
- ARIZ. REV. STAT. ANN. § 13-2316 (1989)
- ARK. CODE ANN. §§ 5-41-101 to 5-41-107 (Michie Supp. 1991)
- CAL. PENAL CODE § 502 (West Supp. 1992)
- COLO. REV. STAT. §§ 18-5.5-101 to 18-5.5-102 (1986 & Supp. 1992)
- CONN. GEN. STAT. ANN. §§ 53a-250 to 53a-261 (West 1985)
- DEL. CODE ANN. tit. 11, §§ 931 to 939 (1987 & Supp. 1993)
- FLA. STAT. ANN. §§ 815.01 to 815.07 (West Supp. 1993)
- GA. CODE ANN. §§ 16-9-91 to 16-9-94 (1992)
- HAW. REV. STAT. §§ 708-890 to 708-893 (Supp. 1992)
- IDAHO CODE §§ 18-2201 to 18-2202 (1987)
- ILL. ANN. STAT. Ch. 38 para. 16D-1 to 16D-7 (Smith-Hurd Supp. 1992)
- IND. CODE ANN. §§ 35-43-1-4 & 35-43-2-3 (Burns Supp. 1992)
- IOWA CODE ANN. §§ 716A.1 to 716A.16 (West Supp. 1992)
- KAN. STAT. ANN. § 21-3755 (1988)
- KY. REV. STAT. ANN. §§ 434.840 to 434.860 (Michie/Bobbs-Merrill 1985)
- LA. REV. STAT. ANN. §§ 14:73.1 to 14:73.5 (West 1986 & Supp. 1993)
- ME. REV. STAT. ANN. tit. 17-A, § 357 (West 1983 & Supp. 1992)
- MD. ANN. CODE art. 27, § 146 (Supp. 1991)
- MASS. GEN. L. Ch. 266, § 30 (1990)
- MICH. STAT. ANN. § 28.529 (Callaghan 1990)
- MINN. STAT. ANN. §§ 609.87 to 609.891 (West 1987 & Supp. 1992);
- MISS. CODE ANN. §§ 97-45-1 to 97-45-13 (Supp. 1992)
- MO. REV. STAT. §§ 537.525, 569.093 to 569.099 (1986 & Supp. 1991);
- MONT. CODE ANN. §§ 45-2-101, 45-6-310 to 45-6-311 (1991);
- NEB. REV. STAT. §§ 28.1343 to 28.1348 (Supp. 1991);
- NEV. REV. STAT. ANN. §§ 205.473 to 205.491 (Michie 1992);
- N.H. REV. STAT. ANN. §§ 638:16 to 638:19 (1986);
- N.J. STAT. ANN. §§ 2C:20-23 to 2C:20-34 (West Supp. 1992);
- N.M. STAT. ANN. §§ 30-45-1 to 30-45-7 (Michie Supp. 1989);
- N.Y. PENAL LAW §§ 156.00 to 156.50 (McKinney 1988);
- N.C. GEN. STAT. § 14-453 to 14-457 (1986);
- N.D. CENT. CODE ANN. § 12.1-06.1-08 (Supp. 1991);
- OHIO REV. CODE ANN. §§ 2913.01, 2913.81 (Anderson 1993);
- OKLA. STAT. ANN. tit. 21, §§ 1951 to 1958 (West Supp. 1993);
- OR. REV. STAT. §§ 164.125, 164.377 (1991); 18
- PA. CONS. STAT. ANN. § 3933 (Supp. 1992);
- R.I. GEN. LAWS §§ 11-52-1 to 11-52-8 (Supp. 1992);
- S.C. CODE ANN. §§ 16-16-10 to 16-16-30 (Law. Co-op. 1985);
- S.D. CODIFIED LAWS ANN. §§ 43-43B-1 to 43-43B-8 (1983 & Supp. 1992);
- TENN. CODE ANN. §§ 39-14-601 to 39-14-603 (1991);
- TEX. PENAL CODE ANN. §§ 33.01 to 33.05 (West 1989 & Supp. 1992);
- UTAH CODE ANN. §§ 76-6-701 to 76-6-705 (1990);
- VA. CODE ANN. §§ 18.2-152.1 to 18.2-152.14 (Michie 1988 & Supp. 1992);
- WASH. REV. CODE §§ 9A.52.110 to 9A.52.130 (1988);
- W. VA. CODE §§ 61-3C-1 to 61-3C-21 (Supp. 1992);
- WIS. STAT. § 943.70 (Supp. 1992);
- WYO. STAT. §§ 6-3-501 to 6-3-505 (1988)
- States not listed had no computer crime statutes as of January 1995.

Table 2-2-2 shows examples of jurisdiction. This table oversimplifies a very complex process involving Federal and State law, the laws of foreign countries, and international agreements.

Table 2-2-2. Computer Crime Jurisdiction

CRIMINAL ACT	JURISDICTION
Intruder and system in one state	State
Intruder in one state; system in another	Federal
Intruder penetrates a system used in interstate commerce or communications	Federal
Intruder penetrates a Federal system in the United States; intent criminal	FBI; United States Secret Service
Intruder penetrates a Federal system in the United States; intent espionage	FBI; National Security
Foreign citizen penetrates a U.S. system which displays a warning banner; no foreign law in place	Apprehension and adjudication can be pursued through existing treaties
Foreign citizen penetrates a U.S. system which displays a warning banner; foreign law in place	U.S. or Foreign law; by agreement

Jurisdiction is cumbersome; however, processes are in place, both nationally and internationally, to resolve issues. The real problem is determining intent and coordinating jurisdiction in real-time. Policy makers may consider putting detection vehicles in place and providing for consolidated and coordinated apprehension of computer criminals. Early detection and apprehension will reduce potential damage and may serve as a useful deterrent. It may be more effective to table issues of intent until after apprehension. The FBI has taken steps in this direction by establishing a Computer Crime Team, made up of representatives from both the Criminal and National Security Divisions in California.

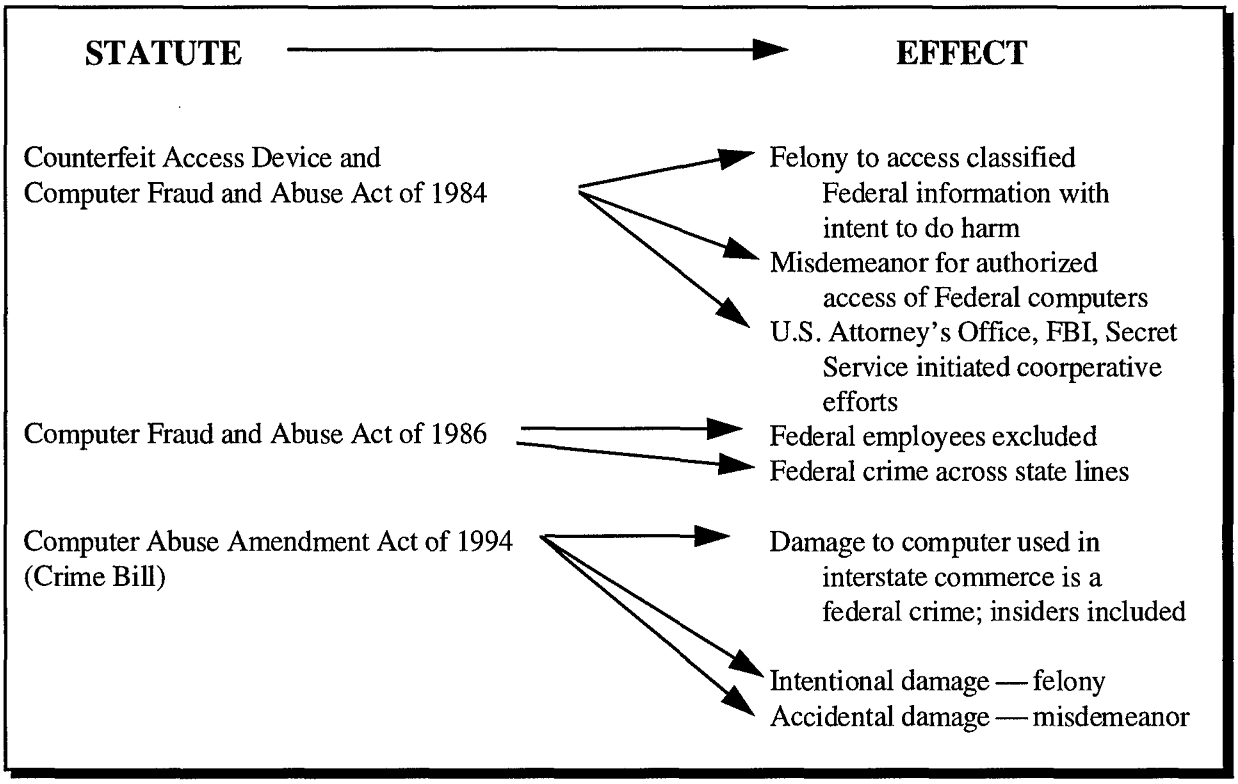
Figure 2-2-10 serves as an illustrative example of the challenges computer crime poses for civil and military law enforcement. Equally informative is the description of the investigative effort associated with the attack on the Air Force's Rome Laboratory in March and April 1994. This effort is detailed in the GAO Report. [GAO]

ARGENTINEAN HACKER

In April 1996, Attorney General Janet Reno announced that DoJ was seeking the arrest of Julio Cesar Ardita, a 21-year old Argentinean university student, for breaking into computer systems belonging to the Navy, NASA, and U.S. universities. Ardita launched his attack on the Navy and NASA from pirated accounts on a Harvard University computer system. He accessed these accounts using various accounts from a service provider in Argentina. When the Navy detected the Ardita intrusion, they sought, in cooperation with the FBI, the first ever computer network (Title III) wiretap. Previous court-ordered wiretaps have authorized wiretapping of telephone lines. This order authorized an automated search of the Harvard University system. The automated nature of the search is key for two reasons. First, an automated tool was necessary to monitor and analyze the 16,000 user account activities to identify the intruder. Second, the automated search protected authorized users from "content monitoring." Content monitoring by a human or humans of the activities of the other 16,000 Harvard account holders would probably have been considered a violation of their privacy and would not have been authorized. Though charges and an arrest warrant were filed in Federal court, the alleged crimes are not covered under an extradition treaty with Argentina and could only be served if Ardita enters the United States or another country which does recognize the alleged computer crime and that has an extradition treaty with the United States. Argentina has cooperated with U.S. authorities, has initiated its own investigation, and may file charges. This case demonstrates the nature of computer crime and the difficulties associated with apprehending a perpetrator. At the same time, it is an encouraging signal that, with the proper tools and processes, law enforcement can successfully investigate and identify intruders, and provide proper evidence for prosecution.

Figure 2-2-10. Example of Challenges Posed by Computer Crime

Figure 2-2-11 portrays the relevant statutes and key effects of each. Acts associated with intellectual property rights, copyright law, and the banking and financial industries are not shown, as they are generally outside the purview of DoD. However, DoD policymakers should keep in mind that government-wide technical solutions and policy must encompass these issues because they are important to the civil agencies of the Federal government and to the private sector.



STATUTE → EFFECT

Counterfeit Access Device and Computer Fraud and Abuse Act of 1984

- Felony to access classified Federal information with intent to do harm
- Misdemeanor for authorized access of Federal computers
- U.S. Attorney's Office, FBI, Secret Service initiated coorperative efforts

Computer Fraud and Abuse Act of 1986

- Federal employees excluded
- Federal crime across state lines

Computer Abuse Amendment Act of 1994 (Crime Bill)

- Damage to computer used in interstate commerce is a federal crime; insiders included
- Intentional damage — felony
- Accidental damage — misdemeanor

Figure 2-2-11. Criminality of Computer Fraud and Abuse

2.2.4 International Legal Environment

Law among nations is not codified in a body of international law. The International Court of Justice recognizes customary international law; that is, law which is common to many nations, as well as international treaties or conventions, such as the Geneva Conventions. Few countries have laws which adequately address computer crime. Among those countries with computer crime statutes, there is no general agreement on the type of conduct that constitutes computer crime. Nor are there any international treaties or conventions which address computer fraud and abuse. Investigation, apprehension, and adjudication of computer criminals, must rely on domestic law and mutual assistance agreements in the form of bilateral and multilateral treaties and agreements. Generally, these agreements require *mutual criminality*; that is, an offense must be a crime in both countries for the foreign country to take legal action. Prosecution of international computer criminals can be an unwieldy process complicated by domestic privacy, search and seizure laws, and jurisdictional considerations. Recognizing the problem, and recognizing that international trade is enhanced by trusted electronic communications, the international community has initiated efforts to *harmonize* international law. Both the Organization for Economic Cooperation and Development (OECD) and the Council of Europe have proposed activities that should be criminalized by member nations. The OECD also issued guidelines for the security of information systems. The IITF Security Issues Forum recently recommended the United States adopt these guidelines.

The United States must also consider the potential effect of its IW-D activities on other sovereign nations. Some agreements, such as the INTELSAT agreement, may bound U.S. IW activities, while others such as the North Atlantic Treaty or other regional mutual defense agreements may facilitate activities. The North Atlantic Treaty Organization (NATO), for example, has a Project Lathe Gambit which, among other activities, hosts meetings of computer crime investigators as well as representatives of the military law enforcement and intelligence communities. International organizations in which the United States maintains membership, such as the International Criminal Police Organization (INTERPOL) may also help law enforcement authorities. In May 1996, INTERPOL sponsored a computer crime investigation workshop.

In general, it is difficult to determine how various agreements and organizations may affect defensive information warfare activities. A knowledgeable General Counsel can, however, determine the international implications of specific policies or planned operations. Therefore, to ensure that defensive information warfare activities operate within the bounds and authorities of the international legal environment, a knowledgeable General Counsel should be involved in IW policy formulation, planning, and operations.

Figures 2-2-12 through 2-2-20 summarize key statutes discussed in this section.

COMMUNICATIONS ACT OF 1934

Purpose, General Provisions, Assigned Responsibilities, and Functions

Purpose: The purpose of the Communications Act of 1934 is to regulate interstate and foreign communications by wire and radio in the public interest. The act establishes the Federal Communications Commission, assigns war powers to the President, addresses radio stations operated by foreign governments, and willful or malicious interference with radio transmissions.

General Provisions:

- Established the Federal Communications Commission.
- Unauthorized interception and disclosure of communications by wire or radio prohibited.

Assigned Responsibilities and Functions

President:

- War powers:
  - During any war in which the United States is engaged, the President may:
    - Order any carrier to give preference or priority for national defense communications.
    - Employ armed forces to prevent retarding or obstruction of interstate or foreign communications.
  - Upon proclamation that war or threat of war exists, the President may:
    - Amend or suspend rules and regulations pertaining to any stations capable of emitting electromagnetic radiations.
    - Close and remove any emitting device that may serve as a navigational device.
    - Amend rules pertaining to wire communications.
    - Order the closure or government use of wire facilities.
- Policy direction of the development and operation of a National Communications System.
- Coordinating policy, plans, and programs for the mobilization and use of the Nation's telecommunications resources in an emergency.

Office of Management and Budget:

- Serve as President's principal adviser on procurement and management of Federal telecommunications systems.
- Developing policies for the procurement and management of Federal telecommunications systems.
- Final disposition of appeals on frequency assignments made by Secretary of Commerce.

Secretary of Commerce:

- Serve as **President's principal adviser on telecommunications policies** pertaining to the Nation's economic and technological advancement and to the regulation of the telecommunications industry.
- **Advise the Director of the Office of Management and Budget on** the development of **policies relating to the procurement and management of Federal telecommunications systems.**
- **Conduct studies and evaluations concerning** telecommunications research and development and concerning the initiation, improvement, expansion, testing, operation, and use of **Federal telecommunications systems**. Study and report on the impact of the convergence of computers and communications technology. Advise OMB and others of the results of these studies.

Figure 2-2-12. Communications Act of 1934

Secretary of Commerce (Continued)

- **Develop** and set forth in coordination with the Secretary of State and other interested agencies plans, **policies, and programs which relate to international telecommunications issues.**
- **Coordinate telecommunications activities of the Executive Branch**, including interoperability, privacy, security, spectrum use, and emergency readiness.
- **Establish interagency groups and advisory committees** as required.
- Manage electromagnetic spectrum.
- Evaluate and recommend remedial actions for the capabilities of telecommunications resources.
- Instruct Communications Satellite Organization in its role as representative to INTELSAT.

Secretary of State:

- In the conduct of foreign policy, coordinate with and consider Federal Communications Commission's regulatory and policy responsibilities.
- Direct foreign relations with regard to the Communications Satellite Act of 1962.

Federal Communications Commission:

- Regulate interstate and foreign commerce in communication by wire and radio as required by this act, as amended.
- Report annually to Congress information and data that may be considered of value and any specific recommendations as to additional legislation considered necessary or desirable including all legislative proposals submitted to OMB.

Figure 2-2-12. Communications Act of 1934 (Continued)

PRIVACY ACT OF 1974

Purpose, General Provisions, Assigned Responsibilities and Functions

Purpose: The objective of the Privacy Act of 1974 is to protect personal privacy from invasions by Federal agencies, in light of increasing use of information technology in the Federal government and the associated increase in personal information maintained by Federal agencies. The law allows individuals to specify what information may be held by a government agency and gives individuals the right to obtain information held on them by the Federal government.

General Provisions:

- The Act levied civil and criminal penalties for violations of the provisions of the Act.
- The Act requires physical security practices, information management practices, and computer and network controls necessary to ensure individual privacy.

Assigned Responsibilities and Functions:

President:
- Submit an annual report to the Speaker of the House and President pro tempore of the Senate.

Privacy Protection Study Commission:
- Study automation practices and privacy issues at federal, state, and local level.
- Recommend legislation, regulation, and policy to protect individual privacy.

Office of Management and Budget:
- Develop guidelines and regulations.

Federal Agencies:
- Not disclose personal information without written consent or under specified conditions.
- Account for disclosures.
- Upon request, allow individuals access to information maintained on them.
- Minimize records maintained to those required for business.
- Identify how information will be used on forms requesting information.
- Publish in the Federal Record new or revised systems containing personal information.
- Publish rules implementing provisions of the Act.
- Not sell or rent an individual's name and address.
- Notify OMB and Congress in advance of any proposal to establish or alter any system of records.

Figure 2-2-13. Privacy Act of 1974

FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978

Purpose, General Provisions, Assigned Responsibilities and Functions

Purpose: The President may authorize electronic surveillance without a court order to acquire foreign intelligence information in the United States. Other Federal officers, with the approval of the Attorney General, may request court orders for approval to conduct electronic surveillance. Probable cause of criminal activity is not required. Special seven member court is established to authorize surveillances. The Act prescribes the time limits and procedures that must be followed with or without a court order. Terms are defined including minimization procedures which are procedures that must be taken to prohibit the dissemination and minimize the acquisition and retention of nonpublic information gathered on non-consenting United States persons.

General Provisions:

- Targets of electronic surveillance will be agents of foreign powers as defined in the Act.
- Minimization techniques will be used to reduce acquisition of information on United States persons.
- Information acquired concerning a United States person may not be disclosed without consent except in accordance with prescribed procedures.
- Court orders are required; the President, if the situation warrants, may authorize electronic surveillance in accordance with prescribed procedures.
- Grants President limited—15 days—exclusion during time of declared war.
- Assigns criminal and civil liability.

NOTE: Some forms of foreign electronic intrusion might be considered outside of the scope of this act. A foreign power, as defined in Section 1801, must be linked to a foreign government or political organization. International terrorism is an exception to this political or national affiliation but is defined as involving violent acts or acts dangerous to human life. If the Drug Cartels are considered foreign powers under the terms of this Act, then most organized or sponsored electronic intrusions should be as well.

Assigned Responsibilities and Functions

President:

- Authorize, through the Attorney General, electronic surveillance to acquire foreign intelligence information without a court order.

Attorney General:

- Certify in writing, under oath, that the foreign intelligence information to be gathered will likely not acquire communications by United States persons, and that proposed minimization procedures are in accordance with the law.
- Transmit a copy of the certification to the court established by this act.
- Report minimization procedures to the House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence.
- Assess compliance with published minimize procedures to the House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence.
- May direct a specified common carrier aid electronic surveillance efforts. The carrier will be compensated for the aid provided.
- Submit annual reports to Congress regarding the number of applications, orders and extensions.
- Report semiannually on all electronic surveillance under the Act.

Figure 2-2-14. Foreign Intelligence Surveillance Act of 1978

Director of Central Intelligence:

- Provide consultation to the Chief Justice on appropriate security measures for safeguarding the Attorney General certifications under his act.
- Provide consultation to the common carriers on appropriate security measures for safeguarding electronic surveillance operations.

Court Established by this Act:

- Issue court orders based upon requests having met the requirements of this act.
- Maintain requests under security measures established by the Chief Justice with the concurrence of the Attorney General.

Other Federal Officers:

- May make applications for court orders based upon the approval of the Attorney General and certification by a senior Executive Branch official responsible for national security or defense.

Communication Common Carriers:

- Furnish information, facilities, or technical assistance as necessary and as directed by the Attorney General. Carriers will be compensated for support rendered.
- Maintain secrecy of the operation and records.

Figure 2-2-14. Foreign Intelligence Surveillance Act of 1978 (Continued)

ELECTRONIC COMMUNICATIONS PRIVACY ACT OF 1986

Purpose, General Provisions, Assigned Responsibilities and Functions

Purpose: To update Federal privacy provisions; incorporating new technology and capabilities.

General Provisions:

- The definition of electronic communication system includes and wire, radio, electromagnetic, photooptical or photoelectronic facilities for the transmission of electronic communications, and any computer facilities for the electronic storage of communications.
- "Communications Common Carriers" is changed to "providers of wire or electronic communication" services.
- Remains legal to intercept electronic communications that are readily accessible to the general public unless such interception causes interference to lawful receivers.
- Authorizes civil damages for the any person whose wire, oral, or electronic communications is illegally intercepted, disclosed, or used.
- The act does not prohibit the interception of encrypted or other executive branch official communications by authorized officers of the government for communications security or for under the Foreign Intelligence Surveillance Act of 1978.
- Penalties are levied against those divulging the plan or existence of a legal surveillance.
- The Attorney General may request an injunction against anyone who is engaged or plans to engage in a felony violation of this act.
- Unlawful access or divulgence of electronically stored communications or electronic communicate service or remote computing service is illegal.
- Government entities may request a court order to require service providers to make a backup copy of records or communications.
- Court orders are required for pen registers or trap and trace devices except for normal carrier operations and maintenance or with user authorization.
- Intentional or malicious interference with the operation of a communications or weather satellite is illegal.

Assigned Responsibilities and Functions:

Attorney General:

- Annually report to Congress on the number of pen register/trap and trace orders requested by law enforcement agencies of the Department of Justice.

Federal Bureau of Investigation:

- May request subscriber information, toll billing and transactional records with written certification that the information is relevant to a foreign counterintelligence investigation or that the individual is an agent of a foreign power as defined in the Foreign Intelligence Surveillance Act of 1978.
- The FBI may disseminate obtained information to other government agencies with relevant responsibilities.
- The Director of the FBI will report to the House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence semiannually on these requests.

Figure 2-2-15. Electronic Communications Privacy Act of 1986

COMPUTER SECURITY ACT OF 1987

Purpose, Assigned Responsibilities and Functions

Purpose: To improve the security and privacy of sensitive information in Federal computer systems by establishing minimum acceptable security practices. The act emphasizes risk-based, cost-effective security and establishes the Computer System Security and Privacy Advisory Board within the Department of Commerce.

Assigned Responsibilities and Functions

President:
- Disapprove or modify standards and guidelines published by the Secretary of Commerce pertaining to Federal computer systems. This authority may not be delegated.

Office of Personnel Management:
- Issue regulations prescribing procedures and scope for training of Federal civilian employees.

Secretary of Commerce:
- Promulgate compulsory and binding standards and guidelines pertaining to Federal computer systems.
- Waive, in writing, compulsory or binding standards if it can be proven that compliance would adversely effect mission accomplishment of a Federal computer system.
- Notice of waiver must be transmitted to Committee on Government operations of the House of Representatives and the Committee on governmental Affairs of the Senate
- Limitations: Authority is subject to direction by the President and Office of Management and Budget.

National Institute of Standards and Technology:
- Responsible for developing standards and guidelines for Federal computer systems including cost-effective security and privacy of sensitive information.
- NIST should draw upon the technical advice and assistance, including work products, of the National Security Agency.
- Submit standards and policies to the Secretary of Commerce for promulgation along with recommendations as to the extent they should be made compulsory or binding.
- Develop guidelines for training employees in security awareness and practices.
- Assist the private sector, upon request.
- Make recommendations to GSA on policies and regulations.
- Provide technical assistance to operators in implementing standards and guidelines.
- Ensure, to the maximum extent possible, that standards for sensitive information are consistent and compatible with standards for classified information.

General Services Administration:
- Revise Federal information resource management regulations to be consistent with standards and guidelines promulgated by the Secretary of Commerce.
- Limitations: Authority is subject to direction by the President and Office of Management and Budget.

Figure 2-2-16. Computer Security Act of 1987

Federal Agencies:

- May promulgate standards for cost-effective security and privacy of sensitive information that are more stringent than standards promulgated by the Secretary of Commerce, as long as, compulsory and binding provisions are included.
- Provide mandatory periodic training for all persons involved in management, use, or operation of Federal computer systems containing sensitive information.
- Identify each Federal computer system which contains sensitive information.
- Establish security plans for each system identified above and provide copies to NIST and NSA.

Federal Computer System Operators:

- Establish security plans for all computer systems that contain sensitive information.

Computer System Security and Privacy Advisory Board:

- Identify emerging issues relative to computer systems security and privacy.
- Advise NIST and Secretary of Commerce on security and privacy issues pertaining to Federal computer systems.
- Report findings to the Secretary of Commerce, the Director of the Office of Management and Budget, the Director of the National Security Agency and appropriate committees of Congress.

Figure 2-2-16. Computer Security Act of 1987 (Continued)

COMMUNICATIONS ASSISTANCE FOR LAW ENFORCEMENT ACT OF 1994
(Digital Telephony Act)
Purpose, General Provisions, Assigned Responsibilities and Functions

Purpose: To make clear a telecommunications carrier's duty to cooperate in the interception of communications for law enforcement purposes, and to ensure that current and future networks and equipment (digital) are wiretap-friendly. The goal is to ensure continued capability and capacity to support legal wiretaps.

General Provisions:

- Law enforcement agency cannot require any specific design of equipment or facilities.
- Requirements do not apply to information service providers or private networks and interconnection services and facilities.
- Carriers are not responsible for decrypting communication unless the encryption is provided by the carrier and the carrier is capable of decrypting.
- Cordless telephones and modulation techniques "the essential parameters of which have been withheld from the public with the intention of preserving the privacy of such communication." are included under the "expectation of privacy" clause. Unauthorized interception is illegal.

Assigned Responsibilities and Functions:

Attorney General:

- Establish capacity requirements for the number of simultaneous interceptions, pen registers, and trap and trace devices.
- Reimburse carriers for costs directly associated with modifications necessary to comply with the act.

Federal Communications Commission:

- Prescribe rules necessary to implement the act.

Telecommunications Carriers:

- Shall ensure that its equipment or facilities that provide customer services are capable of isolating and interception and providing call-identification of all wire and electronic communications.
- Ensure activation of this capability is restricted to court order or other lawful authorization.

Figure 2-2-17. Communications Assistance for Law Enforcement Act of 1994

VIOLENT CRIME CONTROL AND LAW ENFORCEMENT ACT OF 1994
TITLE XXIX--COMPUTER CRIME
Purpose, Impact and General Provisions

Purpose: Title XXIX of the 1994 Comprehensive Crime Bill is cited as the Computer Abuse Amendments Act of 1994. It amends Section 1030 of Title 18; the computer crime statute.

Impact of 1994 Amendments:

- Includes insiders who exceed their authorized access and cause damage. Previous statute excluded insiders. Legislators feared that it might be used against whistle-blowers.
- Trespass of any computer used in interstate commerce or communications is a federal crime.
- Civil action can be taken by victims of computer crime.
- Language protecting federal interest computers and foreign commerce was accidentally deleted. See (a)(5)(A) and (a)(5)(B) below. Until corrected, if the intent of an intrusion is not espionage, unauthorized access of a government computer is punishable by 1 year for the first offense, and 10 years for the second. No special provisions are made for damage to government computers.

General Provisions of Section 1030:

- Secret Service, in addition to other agencies, has authority to investigate offenses under this section.
- A Federal interest computer is one used exclusively by a financial institution or the U.S. Government or a computer that, if not exclusively used by the above, the intrusion impacts the operations of a financial institution or the Government.
- Offenses punishable under this section include:
  - National Security Information: (a)(1) Anyone who knowingly accesses, without authorization or exceeding authorization, to obtain national defense, foreign relations or restricted information protected by statute or Executive Order if the information is to be used to injure the U.S. or give advantage to a foreign government. (10 years first offense; 20 years second offense)
  - Financial Records: (a)(2) Intentional access, by anyone without authorization or exceeding authorization, to obtain financial records. (1 year first offense; 10 years second offense)
  - Government Computers: (a)(3) Intentional access of a computer used exclusively by the Government or, if not exclusively for Government use, the access adversely affects the Government's use of the computer. (1 year first offense; 10 years second offense)
  - Fraud: (A)(4) Knowingly and with intent to defraud accesses a Federal interest computer. (5 year first offense; 10 years second offense)
  - Intentional Damage: (a)(5)(A) Knowingly transmits computer code or commands with the intent to damage an interstate communications or commerce computer. (5 years first offense; 10 years second offense)
  - Unintentional Damage: (a)(5)(B) Knowingly transmits computer code or commands with reckless disregard of the risk that it may damage an interstate communications or commerce computer. (1 year)
  - Password Trafficking: (a)(6) Knowingly, and with intent to defraud, traffics in passwords that may affect computers used by or for the U.S. Government or interstate or foreign commerce. (1 year first offense; 10 years second offense)

Figure 2-2-18. Violent Crime Control and Law Enforcement Act of 1994

National Defense Authorization Act for Fiscal Year 1996
Section 1053 (Kyl Amendment)
Purpose, Assigned Responsibilities, and Functions

Purpose: To have the President review the national policy on protecting the national infrastructure against strategic attacks.

General Provisions: Due to its brevity and significance, Section 1053 is provided verbatim below:

Sec. 1053. REPORT OF NATIONAL POLICY ON PROTECTING THE NATIONAL INFORMATION INFRASTRUCTURE AGAINST STRATEGIC ATTACKS

Not later than 120 days after the date of the enactment of this Act, the President shall submit to Congress a report setting forth the results of a review of the national policy on protecting the national infrastructure against strategic attacks. The report shall include the following:

(1) A description of the national policy and architecture governing the plans for establishing procedures, capabilities, systems, and processes necessary to perform indications, warning, and assessment functions regarding strategic attacks by foreign nations, groups, or individuals, or any other entity against the national information infrastructure.

(2) An assessment of the future of the National Communications Systems (NCS), which has performed the central role in ensuring national security and emergency preparedness communications for essential United States Government and private sector users, including a discussion of—

(A) whether there is a Federal interest in expanding or modernizing the National Communications System in light of the changing strategic national security environment and the revolution in information technologies; and

(B) the best use of the National Communications System and the assets and experience it represents as an integral part of a larger national strategy to protect the United States against attack on the national information infrastructure.

Figure 2-2-19. Kyl Amendment

TELECOMMUNICATIONS ACT OF 1996

Purpose, General Provisions, Assigned Responsibilities, and Functions

Purpose: To provide for a pro-competitive, de-regulatory national policy framework designed to rapidly accelerate private sector deployment of advanced telecommunications and information technologies and services to all Americans by opening telecommunications markets to competition.

NOTE: This Act is detailed and lengthy. General Provisions and Responsibilities and Functions below have been selected for their possible relevance to the DoD.

General Provisions:

- Telephone Service:
  - Amends the Communications Act of 1934 to establish a general duty of telecommunications (long-distance) carriers to interconnect directly or indirectly with the facilities and equipment of other carriers and not to install any network features that would limit interoperability.
  - Requires local exchange carriers to allow resale of their services at wholesale rates, allow access to their facilities, and to otherwise take actions that facilitate local competition.
- Telecommunications Equipment Manufacture:
  - Permits Bell Operating Companies to manufacture telecommunications equipment and participate in research and development.
- Broadcast Services:
  - Relaxes multiple ownership rules.
- Cable Services:
  - Removes rate caps.
- Regulatory Reform
  - Limits FCC and State regulation which is no longer necessary or that restricts competition
- Obscenity and Violence
  - Prohibits obscene or harassing phone calls or other electronic transmissions; e.g., Facsimile or electronic mail.

Assigned Responsibilities and Functions:

Federal Communications Commission:

- Establish regulations to implement the requirements of the Act.
- Institute a Federal-State Board to recommend changes to FCC regulations.
- Establish procedures for oversight of coordinated network planning by carriers.
- Participate in the development of industry standards.

Figure 2-2-20. Telecommunications Act of 1996

2.3 REGULATORY ENVIRONMENT

WHAT'S NEW?

This section now revised to addresses the following:

- EO 12958.
- FCC Rule Making Process.
- FCC Open Network Architecture.
- Summaries of EO 12382, 12958, and the new EO 13010 on Critical Infrastructures.

2.3.1 Introduction

The Federal government regulates industry and Federal information warfare activities in three ways:

- By passing laws and issuing orders and regulations.
- Through the activities of regulatory agencies.
- Through export control.

2.3.2 Orders and Regulations

This section addresses orders and regulations. Executive Orders are formal policy documents issued by the President of the United States. Normally, Executive Orders either precede or implement law. They are published in the U.S. Code of Federal Regulations and, unless classified, are frequently reprinted with relevant statutes in the U.S. Code Annotated. Other documents such as Presidential Proclamations, Memoranda, and Directives are equally formal but have more specialized functions. Orders and regulations are issued to achieve some of the same basic goals of legislation:

- To ensure the availability of telecommunications infrastructure, particularly for national defense purposes.
- To regulate the communications facilities in the public interest.
- To provide access to governmental documents.
- To protect certain classes of information from unauthorized disclosure (for example, classified information).
- To preserve individual privacy.
- To define the limits of authorized and unauthorized behavior.
- To define administrative responsibility.

Several Executive Orders have established policy and procedures and assigned responsibility for Federal information security. Executive Order 12333 is significant because it makes the Secretary of Defense the Executive Agent for signals intelligence and COMSEC for the Federal government. NSA executes this responsibility on behalf of the Secretary of Defense. Executive

Order 12356 gives responsibility for overall policy direction on national security information to the NSC and establishes the ISOO under the GSA to develop directives to implement the order and oversee compliance. Executive Order 12958 revoked Executive Order 12356 and placed greater responsibility for security on OMB. These assigned roles and responsibilities complement those assigned by statute for privacy and Federal information security and are depicted in Figures 2-2-5 and 2-2-7 in Section 2.2, Legal Environment. Parentheses are used to depict these assignments of non-statutory responsibilities.

Executive Order 12472 assigns responsibilities for telecommunications to support NS/EP. Recognizing the need for industry feedback in NS/EP activities, Executive Order 12382 establishes the NSTAC. In addition to its role as a presidential advisory committee, meetings between the NSTAC and the NCS Committee of Principals (COP) serve as useful forums for exchange of information between industry and government. Appendix A includes a summary of the NSTAC organization and roles. An outgrowth of the NSTAC, the Network Security Information Exchange (NSIE) serves as a valuable forum for information exchange between industry representatives. Assigned NS/EP responsibilities are depicted in Figure 2-2-6 in Section 2.2, Legal Environment. Parentheses are used to depict these assignments of non-statutory responsibilities.

Recently, the Critical Infrastructures Working Group recommended the establishment of a Presidential Commission on Critical Infrastructure Protection. [CIWG] Executive Order 13010, signed on 15 July 1996, to implement the recommendations of the Working Group is shown at Figure 2-3-7.

The U.S. Code of Federal Regulations (CFR) is a codification of the general and permanent rules published in the Federal Register (FR) by the Executive departments and agencies of the Federal government. The CFR describes the legislative basis, goals, and predominant policies of the Federal government. In effect, it implements law and Executive Orders. Agency instructions are published along with *Action* sections identifying requirements for Federal agencies. Unless otherwise noted, Federal regulations published in the CFR after notice and comment are binding on both the government agencies and those regulated by the agencies. Many titles and chapters are relevant to defensive information warfare; Regulatory Documents, Appendix B, Reference, provides a sampling of exemplary sections.

It is unlikely that policymakers will target the CFR to make significant changes in Federal operations. The FCC rulemaking process may be an exception; policy makers might want to monitor FCC rule making as it implements the competitive environment mandated by the Telecommunications Act of 1996. The CFR does, over time, reflect legal and regulatory changes in the form of implementing regulations. As a reference, therefore, the CFR is useful as it is a readable and comprehensive compilation of existing macro- and micro-Federal guidance.

As a final note, the Uniform Commercial Code (UCC), which is relevant to IW-D primarily in the area of electronic commerce, is applicable to both civil agencies and the private sector. The UCC standardizes state laws relating to sales and secured transactions. Sponsored by the National Conference of Commissioners on Uniform State Laws and the American Law Institute, the UCC has been adopted by virtually all states (with some amendment) but has not been adopted by the Federal government. Federal commercial law and Federal and state regulatory law override the UCC.

2.3.3 Regulatory Agencies

Several regulatory agencies potentially affect the information infrastructure. The FCC is an independent regulatory agency established to regulate the telecommunications industry. The DoJ also has a regulatory role in the telecommunications industry; it enforces antitrust laws. Other independent agencies, such as the Federal Trade Commission (FTC), the Interstate Commerce Commission (ICC), and the Nuclear Regulatory Commission, can have secondary effects on the PSN. As discussed in Section 2.1, dependencies exist among the nation's infrastructures. Figure 2-1-4 depicts agencies and organizations with interests and responsibilities, including regulation, for critical infrastructures. For example, the Nuclear Regulatory Commission requires utilities to maintain constant communications to nuclear power plants. If isolated, the power plants are required to cease operations. Utilities maintain robust connectivity over private and public systems to these facilities to prevent isolation. It is conceivable that an attack on the power distribution infrastructure could be launched over the PSN. Loss of power would seriously impact the information infrastructure.

The remainder of this section will focus on the FCC and its role in ensuring the reliability and availability of the telecommunications infrastructure.

The FCC was established by Congress as an independent regulatory agency. The FCC affects information assurance formally by issuing orders regulating the telecommunications industry and informally by generating consensus and exchanging information. While the Communications Act of 1934, as amended, does not assign the FCC a national security role, it is responsible for ensuring the reliability of the PSN. After the large-scale PSN outages in 1990, the FCC issued reliability regulations which, though limited in scope, levied reporting requirements on long-haul carriers and established the Network Reliability Council (re-chartered as the Network Reliability and Interoperability Council [NRIC] in 1995) to study and report on PSN reliability.

Effective April 6, 1992, the FCC added Section 63.100 [USCFR] to its rules requiring common carriers (local exchange and interchange carriers) to promptly notify the FCC of any outage that lasts longer than 30 minutes and that potentially affects 50,000 or more customers. Subsequent rule changes require telephonic follow-up to record copy notification of FCC Watch Officers located in Washington, DC, and Grand Island, NE.

The NRIC is a Federal advisory committee that exchanges information, and considers PSN reliability issues. It consists of senior telecommunications industry representatives and federal, corporate, and private customer representatives. The NCS is represented on the Council. The NRIC studies PSN outages and reports its findings. Early NRIC reports, for example, indicated that, historically, backhoes have been the principal enemy of the PSN. These reports resulted in the "Call Miss Utility" publicity campaign. The Congress considered levying criminal penalties for negligence in digging. Through forums such as the NRIC, NSTAC, and other advisory committees, the government can influence cooperation within industry and identify priorities to senior industry representatives. Advisory Committees, Appendix A, includes an organizational summary for the NRIC.

The Telecommunications Act of 1996 charges the FCC with publishing regulations necessary to implement the Act. Because of the contentious political environment surrounding the Act (almost 1 year of vigorous debate, aggressive lobbying, advertising, and over 50 amendments) many of the specifics necessary to actually implement the competitive environment called for in the Act were left to the FCC. The manner in which the Act is implemented may have significant impact on the long-term reliability and availability of the public network.

The following brief account highlights the major components of the standard FCC rulemaking process. FCC rules and regulations are subject to a public notice and comment process similar to that required for other federal regulations. Major changes to the rules are presented to the public as either a Notice of Inquiry (NOI) or Notice of Proposed Rule Making (NPRM). The commission will issue an NOI when it is simply asking for information on a broad subject or trying to generate ideas on a given topic. An NPRM is issued when there is a specific change to a rule being proposed. If an NOI is issued, it must be followed by either an NPRM or Memorandum Opinion and Order (MO&O). When an NOI or NPRM is issued, the public can comment initially and respond to the comments that are made. An oral argument before the Commission may be needed to allow the public to testify as well as to allow FCC bureaus and offices to present diverse opinions. Subsequent to the public comment, a Report and Order is issued by the Commission stating the new or amended rule. Petitions for Reconsideration may be filed by the public within 30 days of the issuance of a rule. The Commission may issue an MO&O based upon its review of Petitions for Reconsideration. FCC proceedings are published in the Federal Register which is available in Public Libraries and can be found on-line from the Government Printing Office directly or through Federal Depository Library Gateways.

Of particular interest to the NS/EP community is the long-term impact on reliability and availability of the FCC's Open Network Architecture (ONA). ONA is a long-term, evolving process rather than a definitive architecture. It is not applicable to all carriers, though a Comparatively Efficient Interconnection (CEI) requirement is generally equivalent. This discussion will not attempt to address the differences between the ONA and CEI or the carriers excluded from the ONA requirements. It will assume that all carriers, including new common carriers joining the future marketplace as a result of the Telecommunications Act of 1996, are subject to the ONA.

First ordered by the FCC in 1986, the ONA requires carriers to provide independent Enhanced Service Providers (ESP) access to the carriers' basic communications services on an equal basis and cost as the carriers' own enhanced service organizations. Enhanced services include such capabilities as call back, voice mail, call forwarding, digital transmission service and caller identification. For an ESP to provide these enhanced services, it must have real-time access to the common carriers' network elements. The *bottom line* concern of some members of the NS/EP community is stated by the National Research Council:

> First, ONA increases greatly the number of users who have access to network software. In any given universe of users, some will be hostile. By giving more users access to network software, ONA will open the network to additional hostile users. Second, as more levels of network software are made visible to users for purposes of affording parity of network access, users will learn more about the inner workings of the network software, and those with hostile intent will learn more about how to misuse the network. [NRC]

Specific vulnerabilities potentially introduced by ONA include:

- Increased potential for unauthorized access to network elements if strong access control mechanisms are not used.
- Increased access, with increased potential for unauthorized access, to network data.
- Increased distributed intelligence (to customer premises equipment and network elements other than network switches). Distributed intelligence may introduce vulnerabilities.
- Weaknesses associated with an ESP's or common carrier's network.
- Undesirable feature interaction caused by a larger number of enhanced features. [NIST]

ONA evolution can be monitored through the FCC rulemaking process. It will be important to ensure that network security considerations are granted equal footing with the creation of free market conditions.

2.3.4 Export Control

The Department of State (DoS) and the Department of Commerce (DoC) share authority for export control. The Arms Export Control Act of 1968 makes the DoS responsible for the export of items that are primarily for military use. The DoS maintains the International Traffic in Arms Regulations (ITAR) and a Munitions List. Items on the list require a DoS license for export; licenses are granted on a case-by-case basis. The act charges the DoD with providing recommendations to the DoS. The Export Administration Act of 1979 and the Export Administration Regulations (EAR) give the DoC responsibility for export of sensitive or dual-use products, including software and scientific data. The DoC maintains a Commerce Control List (CCL) listing controlled items. There is some overlap between the CCL and the DoS Munitions List, particularly with high technology. Generally, the DoS has purview over technology exports unless it delegates responsibility to the DoC. Figure 2-3-1 depicts these responsibilities for export control.

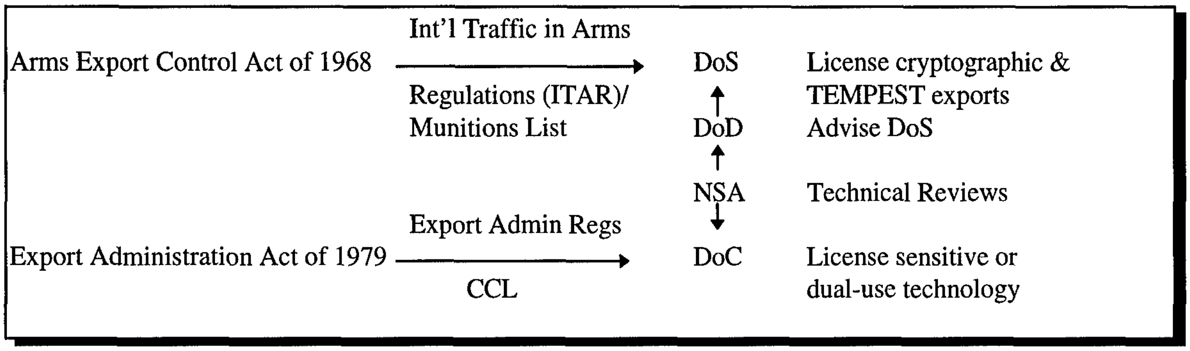


Figure 2-3-1. Export Control Responsibilities

Export of cryptography is a very controversial issue. In attempting to resolve the controversy, policymakers must consider national security, foreign policy, and national and international market forces. See Section 2-4, Policy, for a more detailed discussion of encryption export control issues.

Figures 2-3-2 through 2-3-7 summarize the purpose and assigned responsibilities of:

- Executive Order 12333, United States Intelligence Activities.
- Executive Order 12356, National Security Information.
- Executive Order 12382, President's National Security Telecommunications Advisory Committee.
- Executive Order 12472, Assignment of National Security and Emergency Preparedness Telecommunications Functions.
- Executive Order 12958, Classified National Security Information.
- Executive Order 13010, Critical Infrastructure Protection.

Summaries of other relevant Executive Orders are provided in the form of annotated bibliographies in Regulatory, Appendix B, Reference.

EXECUTIVE ORDER 12333
UNITED STATES INTELLIGENCE ACTIVITIES
December 4, 1981
Purpose, Assigned Responsibilities and Functions

Purpose: Ensure the President and National Security Council are provided with necessary information to base decisions concerning foreign, defense, and economic policy and the protection of United States national interests from foreign security threats. Special emphasis should be given to detect and counter-espionage directed against government, corporations, establishments, or persons.

Restrictive Clauses:

- Agencies will not use electronic surveillance techniques except in accordance with procedures established the Attorney General.
- CIA cannot engage in electronic surveillance within the United States except for the training, testing, or as countermeasures to hostile electronic surveillance.
- Counterintelligence definition specifically excludes communications security activities.

Assigned Responsibilities and Functions:

Secretary of Defense:

- Executive Agent for signals intelligence and **communications security of the Federal government.**
- Collect military foreign intelligence and counterintelligence.
- **Provide for the timely transmission of critical intelligence within the U.S. government.**
- **Protect the security of Department of Defense installations, activities, property, information** and employees by appropriate means.

National Security Agency:

- Establish and operate an effective organization for signals intelligence.
- **Execute Executive Agent responsibilities for communication security of the Federal government**
- Conduct research and development in signals intelligence and communications security.
- Conduct foreign cryptologic relationships.

Foreign Intelligence Elements of the Armed Forces:

- "Collection of national foreign intelligence, not otherwise obtainable, outside the United States shall be coordinated with the CIA, and such collection within the United States shall be coordinated with the FBI."

Department of Energy:

- When requested, support NSA communications security activities.

Director of Central Intelligence:

- Primary advisor to President and NSC on national foreign intelligence.
- Develop objectives and guidance for the intelligence community.
- **Advise Secretary of Defense concerning communications requirements of the intelligence community.**
- Conduct special activities approved by the President.

Figure 2-3-2. Executive Order 12333

Department of State:

- Overtly collect information relevant to foreign relations.

Department of Treasury:

- Overtly collect foreign financial and monetary information.

Federal Bureau of Investigation:

- "Within the United States conduct counterintelligence and coordinated counterintelligence activities of other agencies..."
- Support communications security activities of the Federal government when requested by the Director of NSA.

Agencies of the Intelligence Community:

- May provide specialized equipment, technical knowledge, or assistance of expert personnel to support law enforcement activities.

Figure 2-3-2. Executive Order 12333 (Continued)

REVOKED IN APRIL 1995 BY EO 12958 (Figure 2-3-6)

EXECUTIVE ORDER 12356
NATIONAL SECURITY INFORMATION
April 1, 1982
Purpose, Assigned Responsibilities and Functions

Purpose: Prescribes a uniform system for classifying, declassifying, and safeguarding national security information. The order recognizes "that it is essential that the public be informed concerning the activities of its Government, but" certain national defense and foreign relations information must be protected. It specifies the classification levels, authorities, delegation authorities and rules for declassification and downgrading of this information. "Information" is defined as any information or material, regardless of its physical form or characteristics. The order does not address information systems security.

Assigned Responsibilities and Functions:

National Security Council:

- Provide overall policy direction for the information security program.

Administrator of General Services:

- Responsible for implementing and monitoring the program.
- Delegate these functions to the Information Security Oversight Office.

Information Security Oversight Office:

- Develop directives for the implementation of this order.
- Oversee compliance and implementation.
- Conduct on-site reviews.

Federal Agencies:

- Promulgate implementing regulations.

Figure 2-3-3. Executive Order 12356

EXECUTIVE ORDER 12382
PRESIDENT'S NATIONAL SECURITY TELECOMMUNICATIONS ADVISORY COMMITTEE
September 13, 1982
Purpose, Assigned Responsibilities and Functions

Purpose: To establish an advisory committee on National Security Telecommunications.

Assigned Responsibilities and Functions:

National Security Telecommunications Advisory Committee

- Provide information and advice to the president with respect to the implementation of National Security Telecommunications Policy.
- Technical information and advice regarding the feasibility of implementing specific measures to improve national security telecommunications.

Executive Branch Departments

- Provide the Committee with information necessary in carrying out its duties.

Figure 2-3-4. Executive Order 12382

EXECUTIVE ORDER 12472
ASSIGNMENT OF NATIONAL SECURITY AND EMERGENCY PREPAREDNESS TELECOMMUNICATIONS FUNCTIONS
April 3, 1984

Purpose, Assigned Responsibilities and Functions

Purpose: To provide for the consolidation of assignment and responsibility for improved execution of national security and emergency preparedness telecommunications functions.

General Provisions:

- OSTP and the NSC have primary responsibility for implementing this order. They will consult with OMB, FEMA, DoC, DoD, and FCC as appropriate.
- This order establishes the National Communications System (NCS) consisting of the telecommunications assets of the agencies represented on the NCS Committee of Principals (COP). The COP will consist of federal departments, agencies, and entities designated by the President which lease or own telecommunications facilities of significance to national security or emergency preparedness (NS/EP).
- The order assigns wartime and non-wartime emergency functions.

Assigned Responsibilities and Functions:

National Security Council:
- Policy direction for the exercise of war power functions of the President.
- Advise and assist the President in policy, plans, programs, and standards within the Federal government for the identification, allocation, and use of the Nation's telecommunications resources by the Federal during crisis or emergency.
- Policy and oversight for the mobilization of commercial, government, and private telecommunications resources, the NCS, and Federal agency implementation of this order.

Office of Science and Technology Policy:
- Direct the exercise of the war power functions of the President.
- Advice, guidance and assistance to the President and Federal agencies responsible for the provision, management, or allocation of telecommunications resources.
- Establish a Joint Telecommunications Resources Board.
- Recommend to the President on testing, exercising, and evaluating NS/EP capabilities.
- Recommend to the President NS/EP radio spectrum priorities.

Secretary of Commerce:
- Develop radio spectrum plans for Federal government use during crisis or emergency.

Secretary of Defense:
- Serve as the Executive Agent of the NCS.
- Designate a Manager of the NCS.
- Plan, operate and maintain telecommunications services for the National Command Authorities (NCA).
- Ensure NSA plans for security and protection of NS/EP telecommunications.

Secretary of State:
- Plan and provide for a reliable and secure Diplomatic Telecommunications System.

Figure 2-3-5. Executive Order 12472

National Communications System (NCS):

- Assist the President, National Security Council, Office of Science and Technology Policy, and Office of Management and Budget plan for NS/EP communications for the Federal government.
- Serve as focal point for joint industry-government planning and operations.
- Establish a joint industry-government National Coordinating Center.

NCS Committee of Principals:

- Serve as a forum for the review and evaluation of ongoing and prospective NS/EP telecommunications programs.
- Serve as a forum for each agency to report on their ongoing or prospective telecommunications programs in support of NS/EP.

Manager of the NCS:

- Recommend to the Executive Agent and COP an evolutionary architecture, plans to remove or minimize technical impediments to interoperability of government owned or leased telecommunications systems and test and exercise programs.
- Chair the NCS Committee of Principals and provide staff support.
- Implement approved plans or programs.
- Serve as the joint industry-government focal point including technical information concerning the NS/EP telecommunications requirements of the Federal government.

Federal Emergency Management Agency:

- Plan, operate and maintain telecommunications services and facilities to support its emergency management responsibilities.
- Advise State and local governments on NS/EP.
- Provide policy and management oversight of the Emergency Broadcast System.

Central Intelligence Agency:

- Plan, operate, and maintain telecommunications services adequate to support assigned responsibilities and disseminate intelligence within the Federal government.

General Services Administration:

- Ensure Federally owned and managed telecommunications systems meet NS/EP requirements.

Federal Communications Commission:

- Ensure plans for NS/EP communications services are in the public interest, convenient, and necessary.
- Coordinate NS/EP activities with NCS.

Federal Agencies:

- Provide NS/EP requirements, funding, and reports to the Manager of the NCS.

Figure 2-3-5. Executive Order 12472 (Continued)

EXECUTIVE ORDER 12958
CLASSIFIED NATIONAL SECURITY INFORMATION
April 17, 1995
Purpose, Assigned Responsibilities and Functions

Purpose: To prescribe a uniform system for classifying, safeguarding, and declassifying national security information.

General Provisions:

- Two major purposes of the EO are:
  - To prevent unauthorized disclosure of information,
  - To prevent over-classification of information.
- The EO reiterates existing classification policy and establishes a mandatory and systematic declassification process.
- Three levels of classification—Top Secret, Secret, Confidential—are retained.
- Establishes the Information Security Oversight Office (ISOO) within the OMB.
- Establishes the Interagency Classification Appeals Panel.
- Establishes the Information Security Policy Advisory Council

Assigned Responsibilities and Functions:

Director, Office of Management and Budget:
- Issue directives necessary to implement this order in consultation with the Assistant to the President for National Security Affairs and the co-chairs of the Security Policy Board.

Director, Information Security Oversight Office:
- Implement and monitor program on behalf of the Director, OMB.
- Review and approve agency implementing regulations.
- Conduct on-site reviews.
- Prescribe standardized forms and procedures.
- Report annually to the President.

Information Security Policy Advisory Council:
- Recommend changes to policy
- Recommend specific subject areas for declassification
- Serve as a forum to discuss policy issues in dispute.

Agency Heads:
- Notify the President of information proposed to be exempted from automatic declassification.
- Establish controls to ensure that automated information systems, including networks and telecommunications systems that collect, create, communicate, compute, disseminate, process, or store classified information have controls that: (1) prevent access by unauthorized persons; and (2) ensure the integrity of the information.
- Establish controls to ensure that classified information is used, processed, stored, reproduced, transmitted, and destroyed under conditions that provide adequate protection and prevent access by unauthorized persons.

Figure 2-3-6. Executive Order 12958

EXECUTIVE ORDER 13010
CRITICAL INFRASTRUCTURE PROTECTION
15 July 1996
Purpose, Assigned Responsibilities and Functions

Purpose: To develop a strategy for protecting and assuring the continued operation of the following critical infrastructures: telecommunications, electrical power systems, gas and oil storage and transportation, banking and finance, transportation, water supply systems, emergency services (including medical, police, fire and rescue) and continuity of government. Because the infrastructures are privately owned and operated, the government and the private sector must work together to develop a strategy.

General Provisions: The order establishes:

- The *President's Commission on Critical Infrastructure Protection* consisting of representatives from the Executive Branch, State and Local Government, and the Private Sector. The Chair of the Commission will be appointed by the President from outside the government. Not more than two full-time representatives will be appointed by the heads of the following departments and agencies:

  - The Department of the Treasury
  - The Department of Justice
  - The Department of Defense
  - The Department of Commerce
  - The Department of Transportation
  - The Department of Energy
  - Central Intelligence Agency
  - Federal Emergency Management Agency
  - The Federal Bureau of Investigation
  - The National Security Agency

- *The Principals Committee* consisting of:

  - The Secretary of the Treasury
  - The Secretary of Defense
  - The Attorney General
  - The Secretary of Commerce
  - The Secretary of Transportation
  - The Secretary of Energy
  - The Director of Central Intelligence
  - The Director of the Office of Management and Budget
  - The Director of the Federal Emergency Management Agency
  - The Assistant to the President for National Security Affairs
  - The Assistant to the Vice President for National Security Affairs

- *The Steering Committee* consisting of four members appointed by the President. One member shall be the Chair of the Commission and one will be an employee of the Executive Office of the President.

- *The Advisory Committee to the President's Commission on Critical Infrastructures* composed of not more than ten individuals from the private sector appointed by the President.

- *The Infrastructure Protection Task Force (IPTF)* within the Department of Justice, chaired by the Federal Bureau of Investigation, consisting of at least one full-time representative from the FBI, the DoD, the NSA, and part-time assistance from other Executive Branch departments and agencies.

Figure 2-3-7. Executive Order 13010

Assigned Responsibilities and Functions:

The Steering Committee:

- Shall oversee the work of the Commission on behalf of the Principals Committee.
- Shall approve the submission of reports to the Principals Committee.
- Oversee the work of the IPTF

The Principals Committee:

- The Commission reports to the President through the Principals Committee
- Review Commission reports and recommendations before submission to the President.

The Commission:

- Shall identify and consult with public and private sectors, including Congress that own or operate critical infrastructures, contribute to infrastructure assurance, or that may have differing perspectives.
- Shall assess the scope and nature of the vulnerabilities of, and threats to, critical infrastructures.
- Determine and assess legal and policy issues associated with efforts to protect critical infrastructures.
- Recommend a comprehensive national policy and implementation strategy for protecting critical infrastructures from physical and cyber threats.
- Propose statutory and regulatory changes.

The Infrastructure Protection Task Force (IPTF):

- Increase coordination of existing infrastructure protection efforts while the Commission is conducting its analysis and until the President acts on the Commissions recommendations.
- Identify and coordinate existing expertise, inside and outside of the Federal Government, to:
    - Provide, or facilitate and coordinate the provision of, expert guidance to critical infrastructures to detect, prevent, halt, or confine an attack and to recover and restore service.
    - Issue threat and warning notices
    - Provide training and education on methods to reduce vulnerabilities and responding to attacks.
    - Conduct after action analyses
    - Coordinate with pertinent law enforcement authorities.

The Department of Defense:

- Shall provide the Commission and the Advisory Committee with administrative services, staff, others support services, and funds and may, at the Commissions request, contract for the services of nongovernmental consultants.

All Executive Departments and Agencies:

- Shall cooperate with the Commission and the IPTF, provide assistance, information, and advice, and share information about threats and warning of attacks and information about actual attacks to the extent permitted by law.
- Shall, at the Commissions request, request that existing Federal advisory committees consider and provide advice on issues of critical infrastructure protection.

Figure 2-3-7. Executive Order 13010 (Continued)

This page intentionally left blank.

2.4 POLICY ENVIRONMENT

WHAT'S NEW?

The end of this section now includes recent activities in:

- Policy development and implementation.
- Risk management.
- Encryption and export policy.

Particularly as it applies to a government body, policy is defined as a high-level overall plan or course of action intended to influence and determine decisions, actions, and other matters. Policy guidance and documents are generally less permanent than regulatory documents, and carry neither the weight nor the force of law. Policy generally applies to a subset of the population, although universal application is not excluded.

Currently, there is no national policy on information warfare; however, a body of guidance is being created in the Executive Branch. Several policy boards, committees, and working groups have been established to address security policy for the government.

Specific issues falling within the realm of information warfare have been addressed in policy documents as the need has arisen. The DoD has produced most of these policy documents. Other regulatory agencies providing policy include the DoC, the DoJ, and the Department of the Treasury (DoTreas).

Issues relating to information warfare are perceived in various ways at the national level. The DoD clearly has an interest in promoting a coherent, national policy and strategy for information warfare. Other Federal Departments and Agencies with a stake in information assurance may have differing perspectives on how to implement information assurance goals. For example, while the missions of Justice and Treasury are very different, both departments are concerned with the protection of information. Their purpose in protecting that information will be driven by dissimilar motivations and mission requirements, different sets of data sensitivity and criticality, and a great variety of threats and vulnerabilities.

Another key factor which contributes to the complexity of the issue of policy at the national level is the dynamic nature of technology. Information and telecommunications have rapidly converged. New terms, such as information superhighway and global/national/defense information infrastructure have emerged. The evolution of technology, and its concurrent influence on the missions of Federal Departments and Agencies, must be closely observed; appropriate responses in the form of intelligent strategies and policies, cogent investment decisions, and responsive implementation plans must be made. One thing is certain—the technological environment and its impact on information warfare will continue to be dynamic. Policy must be crafted in such a way that changes in technology do not result in major policy changes.

2.4.1 Overview of Existing Policy

Table 2-4-1 summarizes those policy documents within the Executive Branch that may influence the creation of policy for information warfare in DoD. (For a listing of key policy documents, see Appendix B, Policy Document Index.) Most of these documents have been produced within the DoD, reflecting the DoD's greater sensitivity to information warfare. Table 2-4-1 is a representative sample of documents that relates to any aspect of the transmission, storage, or protection of information. Many documents dealing with such topics as personnel security, physical security, communications doctrine and procedures, and security hardware have been excluded. With few exceptions, the handling of intelligence-related information has also been excluded.

Table 2-4-1. Information Warfare Policy Documents

Presidential Directives
National Security Directives/Decision Directives
National Communications Security Committee Policies
OMB Circular
Federal Information Resources Manual (IRM)
OSD, Defense Management Review Decisions, Directives, Standards, Regulations,
Manuals, Handbooks, Indexes, and Instructions
CJCS, National Military Strategy Document, Memoranda of Policy, Instructions, Joint Publications
NSA Policy
Army Regulations
Navy Instructions
Marine Corps Orders/Publications
Air Force Regulations and Instructions

Note: Executive Orders were discussed in Section 2.3, Regulatory

2.4.1.1 Executive Branch Policy

The lack of National-level policy on information warfare is a source of concern for many, particularly for the DoD. There is debate across the Federal government as to whether or not a national policy for information warfare is required, how it should be defined, what its components and boundaries are, and whose responsibility it should be. It is a complex issue at the very least, encompassing many legal and regulatory concepts, and confronting such constitutionally-guaranteed rights as individual privacy.

At the Presidential level, policy has been expressed through such instruments as NSDDs and issuances of the National Security Telecommunications and Information Systems Security Committee and its predecessor organizations, the National COMSEC Committee and the National

Telecommunications and Information Systems Security Committee. For example, NSD 42 stated, as a matter of policy, that "national security systems shall be secured by such means as are necessary to prevent compromise, denial, or exploitation"; established an executive agent and a national manager to implement objectives and policies; and redefined the charter of the NSTISSC to include developing operating policies, procedures, guidelines, instructions, and standards.

Another initiative being fostered at senior levels of the Executive Branch is the support for the so-called information superhighway. Vice President Gore is spearheading administration efforts under the Information Infrastructure Task Force (IITF). The information infrastructure of the future will be a key component of any information warfare strategy or policy, whether at the national level, or in the DoD.

A major factor in the handling of information is the delineation of responsibilities by the Computer Security Act of 1987 for classified and unclassified information. Although the DoD has traditionally placed itself at center stage in the ongoing debate regarding information handling, the act very clearly assigned responsibility for policy formulation for sensitive unclassified information to the DoC. The NIST was delegated the responsibility for sensitive unclassified standards and guidelines. The DoD retained its role for classified information.

A cornerstone document to the security of information is OMB Circular A-130, Security of Federal Automated Information Systems. Revisions to the original document have been made over the past 2 years. The most recent revision of Appendix III addresses security. When proposed, the transmittal letter contained the following language, which reflects current thinking at senior levels in the Executive Branch: "This proposal is intended to guide agencies in securing information as they increasingly rely on an open and interconnected National Information Infrastructure. It stresses management controls such as individual responsibility, awareness and training, and accountability, rather than technical controls." The revision requires better integration of security into program and mission goals, reduces the need for centralized reporting of paper security plans, emphasizes the management of risk rather than its measurement, and revises government-wide security responsibilities to be consistent with the Computer Security Act.

In May 1993, the Secretary of Defense and the Director of Central Intelligence established a Joint Security Commission (JSC) to examine the processes used to formulate and implement security policy in the DoD and the Intelligence Community. In executing its charter, the JSC was guided by the following needs: flexible policies to match threats; consistent and cost-effective policies; fair and equitable treatment of all Americans; and affordable security. The Commission saw current security practices and procedures as complex, costly, and fragmented, and a "profusion of policy formulation authorities" with overlaps and sufficient differences "to create inefficiencies and cause implementation problems." The JSC observed that "the policies and standards upon which the Defense and Intelligence Communities base information systems security services were developed when computers were physically and electronically isolated. As a result, policies and standards:

- Are not suitable for the networked world of today ....

- Were developed based on a philosophy of complete risk avoidance and so do not deal effectively with information systems security as part of a balanced mix of security countermeasures ....
- Do not provide the flexibility needed to address the wide variations among systems in use today and planned for tomorrow.
- Do not differentiate between the security countermeasures needed within and among protected network enclaves and those needed when information must travel to and from less protected or unprotected parts of the infrastructure.
- Are beginning to combine computer science and public key cryptography ....
- Are not capable of responding ... to dynamically evolving information technology."

The JSC recommended the creation of "a joint DoD/DCI security executive committee, and that the committee oversee development of a coherent network-oriented information systems security policy for the Department of Defense and the Intelligence Community that also could serve the entire government." The structure which was put in place was shown in Figure 2-1-7, U.S. Security Policy Board.

The 12-member U.S. Security Policy Board was created under the National Security Council by PDD 29. Below the Board were established a 26-member Security Policy Forum (composed of representatives of other Federal agencies and departments) and a 5-member Security Policy Advisory Board with civilian membership. The Board has subordinate working groups to address such subjects as personnel security, physical security, information classification, system security, training, and policy integration.

The existence of and the work produced by the Board has encountered resistance from those who see an overbearing presence from Defense interests, and an attempt to institute closer relationships between the classified and unclassified environments. The future of the Board and its work, particularly in the area of information systems security, is the subject of some debate.

2.4.1.2 Department of Defense Policy

Considerable effort has been undertaken within OSD and the services to move forward in the information warfare area, including the creation of policy documents. These documents have been written to fulfill the primary mission of DoD, i.e., the execution of national military strategy as directed by National Command Authority. This annex provides programming guidance and priorities to support the force structure required to execute the national military strategy and serves as support documentation for the core C4 capabilities identified in the Defense Planning Guidance.

The Secretary of Defense and OSD have published Regulations, Directives, Manuals, Handbooks, and Instructions which relate either directly or indirectly to information warfare. Most notable among these is DoD Directive TS3600.1, Information Warfare. This directive establishes DoD information warfare policy and assigns responsibilities. It provides the basis for developing policy within DoD and in the services and directs acquisition of systems to meet operational requirements. It specifically assigns responsibility, for example, to the Assistant Secretary of

Defense, for C3I as the primary point of contact for information warfare within DoD; to the Director, NSA, for information purposes in matters relating to technology and system development; and to the Director, DISA, for the protection of the Defense Information Infrastructure (DII). DoDD TS3600.1 is currently being revised. Protection of the DII is the basis for a Memorandum of Agreement between DISA and NSA concerning the Defense-Wide Information Systems Security Program (DISSP).

Secretary of Defense Cheney approved policy documents known as Defense Management Review Decisions (DMRDs), which have relevance to information warfare and information systems. The most well known of these is DMRD 918.

The Chairman, Joint Chiefs of Staff (CJCS), has similarly issued Instructions, Memoranda of Policy (MOPs), and Joint Publications. Joint Publication 1, Joint Warfare, refers to the "information differential." CJCS MOP 30, Command and Control Warfare (C2W) provides joint policy and guidance for both offensive and defensive aspects of C2W. Recent Joint Staff publications include CJCSI 3210.01, *Joint Information Warfare Policy* (U), published in January 1996, and CJCSI 6510.01A, *Defensive Information Warfare Implementation*, dated 31 May 1996.

2.4.2 Military Department and Service Policies

The military departments and Services have been busily engaged in developing and implementing policy for information warfare. Although lacking comprehensive guidance from higher authority, emerging service policy, doctrine, and implementing instructions generally refer to DoD Directive TS3600.1 and CJCS MOP 30.

Efforts of the services appear to be proceeding in the same general direction. There are universal concerns for such items as national-level policy, drafting of doctrine, establishing executive agency responsibilities and an operating structure, staffing, integration of information warfare into traditional missions, acquisition, and training.

The exploration of military department directives in detail is beyond the scope of this paper. Appendix A contains Service organizational summaries which discuss key IW/C2W doctrine and policy.

2.4.3 Implementation Standards, Guidelines, and Procedures

Within the Executive branch of government, there exists a large body of standards, guidelines, and procedures designed to implement policy. As instruments of policy, this guidance is essential to ensure adherence to both the letter and the intent of policies from higher authority. In fact, the traceability of guidance and procedure is made not only to policy, but frequently to law as well.

These standards, guidelines, and procedures generally fall into one of the categories shown in Table 2-4-2. Note the large number of applicable documents. It is not within the scope of this paper to explore the details of the implementing guidance. For a listing of key implementation guidelines, standards, and procedures, see Appendix B, Implementation Guidelines, Standards, and Procedures Index. The index contains a thorough representative sample of documents.

Table 2-4-2. Implementation Guidelines, Standards and Procedures

Number	Type Document
24	National Communications Security (COMSEC) Instructions (NACSI), Information Memoranda (NACSIM), and Emanations Memoranda (NACSEM)
63	National Telecommunications and Information Systems Security Committee/National Security Telecommunications and Information Systems Security Committee (NTISSC/NSTISSC) Issuances
4	Office of Management and Budget Bulletins
	Director, Central Intelligence Directives
36	National Computer Security Center (NCSC) Rainbow Series
33	NIST Special Publications
146	Federal Information Processing Standards Publications (FIPSPUBS)
7	DIA Manuals
2	Compartmented Mode Workstation (CMW) Publications
6	COMSEC Program Publications
9	TEMPEST Program Publications
4	Other Security-relevant Government Publications

2.4.4 Recent Activities

2.4.4.1 Policy Development

Currently, there is no specific national policy on information warfare, information assurance, or information protection. However, a body of related policies and guidance has been or is being created in the Executive Branch. The OMB released its latest revision to Circular A-130, which addresses the security of Federal Information Resources.

The military services have also published or drafted several policy or guidance documents: DA Pam 525-69, Information Operations; the Army C2 Protect Library; FM 100-6, Information Operations; OPNAVINST 3430.26, Implementing Instruction for Information Warfare/Command and Control Warfare (IW/C2W); and AFI 33-207, Information Protection Operations.

2.4.4.2 Risk Management

In February 1994, The Joint Security Commission published a report for the Secretary of Defense and the Director of Central Intelligence; "Redefining Security." The report recommended "using risk management as the underlying basis for security decisionmaking." In September 1994, the White House announced the signing of Presidential Decision Directive (PDD 29). The directive stated that a new security process is required and that the process should be based on sound threat analysis and risk management practices.

The actual incorporation of language requiring risk management has appeared in at least one policy-level document. In April 1995, the Director of Central Intelligence issued a revision to Director Central Intelligence Directive (DCID) 1/7, "Security Controls on Dissemination of Intelligence Information," which explicitly encourages a risk management approach to classifiers of disseminated intelligence information.

While a risk management approach has been mandated by the White House, the community at large is having difficulty in determining how to incorporate risk management into its current processes. Several committees and boards are currently attempting to determine how to apply a risk management approach. The problem in defining a risk management approach is that the "risk avoidance" culture that developed and matured during the "Cold War" is not easily overcome.

Historically, the U.S. Government has used a threat-based approach to develop security policies, standards, practices, and procedures. The Joint Security Commission recognized that in the past, most security decisions have been linked in one way or another to assumptions about threat. These assumptions frequently postulated an all-knowing, highly competent enemy. The Joint Security Commission stated, "*Against this danger, we strove to avoid security risks by maximizing our defenses and minimizing our vulnerabilities.... We used worst case scenarios as the basis for most of our security planning.*" This threat-based approach to security resulted in highly controlled, structured security programs whose procedures are intricate and rigidly enforced (a compliance-based approach).

Risk management requires the evaluation of threats and vulnerabilities and a cost-benefit determination of potential security measures. This cost benefit determination involves assessing the impact of successful attacks on information systems, networks, and other elements of the information infrastructure. A risk management approach will enable the allocation of scarce resources effectively and provide security at an affordable price.

2.4.4.3 Encryption and Export Policy

Encryption policy to include exportability of encryption products is one of the most volatile issues within the Federal government and private industry. Encryption policy has also drawn the attention of the Congress.

There is currently strong debate within the United States about the proper balance between national security, law enforcement, commerce and privacy. Law enforcement and national security agencies would like to maintain tight control over civilian encryption technologies and privacy rights advocates fight to expand their ability to distribute and use cryptographic products as they please.

On May 20, 1996, the Interagency Working Group on Cryptographic Policy issued a draft report; "Enabling Privacy, Commerce, Security and Public Safety in the Global Information Infrastructure." The report presents a vision for developing a cryptographic infrastructure that will protect valuable information on national and international networks. Further, the report outlines a course of action for developing an infrastructure that will protect valuable national information resources on national and international networks. Government and industry must work together to create a security management infrastructure and attendant products that incorporate robust cryptography without undermining national security and public safety. A policy for escrow of cryptographic keys that provides a basis for bilateral and multilateral government agreements is needed so that industry can produce products for worldwide interoperability. Industry will participate in defining algorithms and protocol standards, and will develop key escrow encryption products that are suitable for the protection of both government and private sector information and that will ensure timely, lawful, government decryption access. Government will help set standards for the Key Management Infrastructure (KMI) and deliver a market for robust security products. A KMI infrastructure and attendant key escrow products will provide many benefits, both domestic and internationally, as the United States begins to realize the advantages of the global network for improved commerce, security, and public safety.

In addition to the Administration activities, the Congress has been very active in the encryption policy arena. Several bills are currently being considered. On May 20, 1996, the National Research Council released a report entitled "Cryptography's Role in Securing the Information Society." The report was requested by the U.S. Congress with the charge to: "conduct a comprehensive study of cryptographic technologies and national cryptography policy..."; assessing "the effect of cryptographic technologies on.... national security and law enforcement interests of the United States Government, ...commercial interests of United States industry; and...privacy interests of United States citizens; and...the effect on commercial interests of United States industry of export controls on cryptographic technologies."

The NRC's Committee to Study National Cryptography Policy made the recommendations shown in Table 2-4-3.

Table 2-4-3. National Research Council Cryptography Policy Recommendations

1. No law should bar the manufacture, sale, or use of any form of encryption within the United States.

2. National cryptography policy should be developed by the executive and legislative branches on the basis of open public discussion and governed by the rule of law.

3. National cryptography policy affecting the development and use of commercial cryptography should be more closely aligned with market forces.

4. Export controls on cryptography should be progressively relaxed but not eliminated.

4.1. Products providing confidentiality at a level that meets most general commercial requirements should be easily exportable.

4.2. Products providing stronger confidentiality should be exportable on an expedited basis to a list of approved companies if the proposed product user is willing to provide access to decrypted information upon legally authorized request.

4.3. The U.S. government should streamline and increase the transparency of the export licensing process for cryptography.

5. The U.S. government should take steps to assist law enforcement and national security to adjust to new technical realities of the information age.

5.1. The U.S. government should actively encourage the use of cryptography in nonconfidentiality applications such as user authentication and integrity checks.

5.2. The U.S. government should promote the security of the telecommunications networks more actively. At a minimum, the U.S. government should promote the link encryption of cellular communications and the improvement of security at telephone switches.

5.3. To better understand how escrowed encryption might operate, the U.S. government should explore escrowed encryption for its own uses. To address the critical international dimensions of escrowed communications, the U.S. government should work with other nations on this topic.

5.4. Congress should seriously consider legislation that would impose criminal penalties on the use of encrypted communications in interstate commerce with the intent to commit a federal crime.

5.5. High priority should be given to research, development, and deployment of additional technical capabilities for law enforcement and national security to cope with new technological challenges.

6. The U.S. government should develop a mechanism to promote information security in the private sector.

2.4.4.4 Revised Appendix III to OMB Circular A-130

Appendix III, "Security of Federal Automated Information Resources" revised procedures contained in the original A-130 Appendix III and incorporates requirements contained in the Computer Security Act of 1987 (P.L. 100-235) and responsibilities assigned in applicable national security directives. It requires agency programs to include a minimum set of security controls in general support systems and major applications.

The new Appendix III will guide agencies in securing government information resources as they rely increasingly on an open and interconnected National Information Infrastructure. It requires agencies to ensure that risk-based rules of behavior are established, that employees are trained in them, and that the rules are enforced. The revision also integrates security into program and mission goals, reduces the centralized reporting of security plans, emphasizes the management of risk rather than its measurement, and revises government-wide security responsibilities to be consistent with the Computer Security Act of 1987 and the Paperwork Reduction Act of 1995.

The new version of Appendix III eliminates several requirements from previous versions and adds some new ones:

- There is no longer a requirement for an agency information security official.
- There is no longer a requirement to certify the security controls in sensitive applications.
- There is no longer a requirement for an agency-level information security program; training is now required to be specific for systems.
- The requirement for the performance of formal risk analysis, as an element of an agency information security has been dropped. The requirement is for management of risk rather than measurement of risk.
- There is a new requirement for incident response capabilities at the system level.
- There is a new requirement for the inclusion of a summary of agency security plans in the information resources management plan required by the Paperwork Reduction Act.

2.4.4.5 Moynihan Commission

On April 30, 1994, the President signed legislation appointing the Commission on Protecting and Reducing Government Secrecy. This legislation calls for comprehensive reform designed to reduce the volume of information classified, strengthen the protection of legitimately classified information, and improve current procedures for the granting of security clearances. The Commission met for the first time on January 10, 1995. The Commission consists of 12 members; 4 are Members of Congress, 1 is a senior Executive Branch official, and 7 are from the private sector. The Commission staff includes specialists detailed from the Department of State, the Department of Defense, the Central Intelligence Agency, and the National Security Agency.

The Commission staff is currently investigating issues and soliciting views from government officials, industry representatives, scientists, historians and archivists, journalists, and other interested parties on classification, declassification, and personnel security issues and on how new information technologies will affect the protection and reduction of secrecy for the rest of the decade and the 21st century. The Commission is currently developing a report due by mid-1996. A final report containing the Commission's findings and recommendations is scheduled for release in early 1997.

This page intentionally left blank.

2.5 TECHNOLOGY ENVIRONMENT

WHAT'S NEW?

This section now contains:

- Some examples of growing dependence on information technology from the Bosnia experience.
- A more detailed examination of emerging technologies applicable to information assurance.
- A discussion of some of the applicable research and development activities.

Emerging technology has had, is having, and will continue to have a profound impact on both offensive and defensive information warfare. Emerging technology involves all stages in the processing, transmission, storage, encryption, and protection of information. Technology has also advanced in related areas such as physical security, access controls, and audit techniques. Technology solutions are not limited to either hardware or software, but cover the entire spectrum of potential solutions. In many cases, there is a continuous spiral of development as countermeasures are developed to mitigate vulnerabilities, new methods of attack are discovered, and yet additional countermeasures are required. Many technology solutions have the potential of being used for illicit purposes; that fear has recently been expressed with reference to the Security Administrator's Tool for Analyzing Networks (SATAN).

Governments, individuals, and corporations rely more upon information. As the Tofflers note in their book, *The Third Wave*, we have become an information-based society. As information becomes more available and reliance on that information grows, the effects that could result from the loss of the information become more serious. People and organizations rely upon technology for their daily activities. If a serious and coordinated attack is made upon telecommunications assets, there will be serious effects on the general public as well as the military. The military's ability to conduct effective operations will also be seriously impaired.

This section addresses the fundamental information security requirements, highlights some of technologies used for information security, discusses some of the emerging technologies, and briefly discusses some of the research and development efforts in the area of information security. It does not address technologies that are specifically related to battlefield modernization and tactical warfare; such technologies are predominantly classified. Emerging technologies are being fostered by such efforts as the Joint Warfighters Capability Assessment (JWCA) and research and development in technologies that potentially have long-range information warfare applications.

2.5.1 Fundamental Information Security Requirements and Techniques

Our society, in general, has greater reliance upon information and technology than other societies do. The NII (a subset of which is the DII) is enabled by this technology. Disruptions to the infrastructure, as we have experienced through both natural and manmade disasters, have highlighted our critical reliance on information. During these disruptions, both the psychological effects and the incredible cost of deprivation of information have been felt. Minimizing the effects of disruptions will require improved information protection. Emerging technology has the potential of providing some relief.

Information protection comprises the authenticity, confidentiality, availability, integrity, and nonrepudiation of information being handled within the infrastructure. It requires proper implementation of security features appropriate for individual environments, such as passwords, firewalls, or other countermeasures.

Authentication and encryption are two protection techniques that are evolving quickly on the international level. While these techniques may provide effective measures to ensure confidentiality and integrity of information, they would be rendered useless by a denial of service attack on the information infrastructure. Denial of service attacks prevent the user from accessing the information The information infrastructure is very vulnerable to denial of service attacks. It is difficult to provide ironclad countermeasures against a denial of service attack. A comprehensive risk analysis and implementation of recommended countermeasures are essential to mitigate the risk of exposure to this attack. Many technology advances are developed in reaction to an identified problem, and that may be the case with denial of service attacks.

2.5.1.1 Authentication

Authentication is the verification of the identity of an individual or the source of information. In its simplest form, authentication can be thought of in terms of traditional passwords or a Personal Identification Number (PIN). Authentication of identity can also be achieved by other devices, such as tokens, smart cards, or biometric devices which can be attributed uniquely to one individual. Authentication of the source of information can now be demonstrated through such techniques as the digital signature.

The use of passwords is the simplest method of authentication to implement, as well as being the most acceptable to the general public. But because of applications that can guess and steal passwords (such as those used against the DoD during attacks through the Internet) and because of poor password management on the part of users, the use of passwords to provide secure authentication has been severely compromised. The use of one-time passwords, or similar one-time, encrypted authentication techniques may provide a more secure protection mechanism.

Tokens may also be used to authenticate an identity. The individual must present a card to the system and enter a password, as in the mechanism used for an Automated Teller Machine (ATM). Biometric techniques are by far the most exotic and expensive form of authentication. Their advantage is that they are relatively accurate, and, unless the data base is compromised, they eliminate the vulnerability associated with a compromised password or a lost token. In almost all cases, the inaccuracies yield false negative responses, rather than false positive responses, thus erring on the side of strengthened security. Common biometric authentication techniques include fingerprinting, hand measures, voice identification, and retinal scans.

Digital signatures provide an authentication mechanism that a sender and a receiver of a message can use to verify the identity of the sender of a message, and thus the message integrity. Digital signatures use public key cryptography to associate the sender uniquely with the message.

2.5.1.2 Encryption

Encryption is the transformation of data into a form unreadable by anyone without the appropriate decryption key. Encryption allows secure communications over an otherwise non-secured channel. Many products are currently being implemented that address encryption and/or secure communications using password systems, cards, single-use keys, public key systems, and private/secret key systems.

Some of the encryption systems currently available or being developed include S/KEY, Kerberos, RSA (named after its creators, Rivest, Shamir, and Adleman), Privacy Enhanced Mail (PEM), Pretty Good Privacy (PGP), Digital Encryption Standard (DES), Public Key Cryptography Standards (PKCS), and SKIPJACK. To understand the impact these systems may have on information warfare, it is important to understand the difference between public key and private/secret key systems. Traditional cryptography is based on both the sender and the receiver of a message knowing and using the same private/secret key. A significant problem with private/secret key systems is the secure distribution of the key. Public key systems try to alleviate this key management problem. In a public key system each person has two keys, a public key and a private key. The public key is used to encrypt messages; the private key, to decrypt them. In this way the private key is never transmitted across the network. Public key systems are often significantly slower than private/secret key systems. These systems can be combined; the public key system is used to encrypt a private/secret key, which is used to encrypt a message. Using this methodology, the identity of a sender can be authenticated while the data is protected.

S/KEY is a single-use password authentication system developed at BELLCORE and publicly available on the Internet. The purpose of S/KEY is to prevent network sniffing applications from discovering user passwords. A secret password of the client is used with a seed from the host to generate a sequence of single-use passwords. Only the derived, one-time password crosses the network.

Kerberos is an authentication system designed to prevent password detection within a Kerberos environment or among hosts all fully supporting the Kerberos protocol. Kerberos is based on DES symmetric key encryption and uses a trusted host as an independent source of key verification. The Kerberos trusted host or server contains all the secret keys and must be physically secure. If the host is compromised, so are all of the secret keys.

There are also asymmetric encryption systems such as RSA. SPX is an experimental system that uses RSA. SPX depends on each party having a certifying authority. It uses digital signatures that consist of a token encrypted in the private key of the signing entity and that are validated using the appropriate public key. The public key is obtained under the signature of the trusted certification authority. Parts of the authentication exchange are encrypted to prevent a replay attack.

PEM is an Internet mail standard that has been designed and proposed but not yet officially adopted. It was created to provide secure e-mail and works with current e-mail formats. Currently PEM explicitly supports only DES message encryption and supports both DES and RSA for key management. Trusted Information Systems, Inc. (TIS), has released an implementation of PEM that is intended for individual, not commercial, use. There is no cost for the TIS software.

PGP system is based on RSA but does not require a certifying authority. PGP was developed by Phil Zimmerman who provided it freely, resulting in international distribution and, consequently, in investigations for export violations. The Department of Treasury recently announced that it was no longer investigating Phil Zimmerman for export violations. PGP for individual use is available for the DOS, Macintosh®, UNIX™, Amiga, Atari, VMS, and OS/2® platforms and has Italian, Spanish, German, Swedish, and Russian foreign language modules available. PGP is available via anonymous file transfer protocol (ftp) from sites in the United States, Germany, Sweden, Spain, Canada, United Kingdom, Italy, Finland, Australia, Netherlands, and New Zealand. PGP is also available commercially from ViaCrypt, but this version is not available for export from the United States.

DES is an encryption block cipher defined and endorsed by the U.S. Government. DES is a secret-key, symmetric encryption system. Symmetric key encryption means that the same key is used for encryption and decryption. DES hardware and software export from the United States is strictly regulated by the DoS and NSA. However, the DES algorithm is currently in use worldwide.

PKCS is a set of standards for implementation of public-key cryptography issued by RSA Data Security, Inc., in cooperation with a computer industry consortium. PKCS is compatible with PEM but extends beyond it to handle binary data. It supports RSA, DES, and Diffie-Hellman key exchange.

SKIPJACK, the algorithm used by the Clipper chip, is a classified encryption/decryption algorithm designed by NSA. SKIPJACK uses key escrow. It is designed with a law enforcement access field (LEAF) which enables an authorized law enforcement official to decrypt the data. Reviews of SKIPJACK show it to be significantly more robust (more resistant to breaking) than DES. However, there is significant public concern about the law enforcement access and about the possibility of NSA being able to decrypt messages.

Key escrow involves an escrow agent maintaining a copy of an encryption key that can decrypt otherwise secure data. Law enforcement agencies need to decrypt messages, because otherwise well-financed criminal organizations can secure their communications against monitoring by law enforcement agencies. Key escrow provides for messages to be secure from all unauthorized readers, except for valid law enforcement authorities. This concept is a source of significant public controversy, because there is strong public sentiment against the Government being able to compromise data that the public perceives to be secure. An additional controversy arises when exportation of key escrow is required. U.S. companies attempting to sell computers to foreign entities would be required to sell them with the key escrow feature, which would make the product undesirable to the foreign buyers. Because there are many other methods for encrypting data, the foreign buyers are not limited to considering U.S.-made products if they desire security features.

The export restrictions placed on related hardware and software inhibit widespread implementation of U.S. manufactured authentication and encryption systems. These restrictions discourage commercial application developers from including encryption systems in their products. Not only do the restrictions discourage export of these products, but also encryption is illegal in some countries.

2.5.1.3 Communications

There will soon be a proliferation of high-volume data communications exchange systems. Industry is driving the market and technological advances in increased communications bandwidth. The new technologies that are facilitating higher rates of data communications include Synchronous Optical Networks (SONET), Asynchronous Transfer Mode (ATM), Frame Relay, Broadband Technologies, and Integrated Services Digital Network (ISDN). While these protocols are very different in implementation, they all allow for a dramatic growth in bandwidth. ISDN is primarily intended to provide relatively high data transfer rates to small businesses and home computers; the other protocols are intended for use in Wide Area Networks. Care must be exercised in employing these technologies, as the degree to which security features have been considered and implemented will vary, and vulnerabilities will exist.

SONET is a fiber-based ring technology that, while offering significant bandwidth, is vulnerable to interception. Data messages are transmitted intact throughout the ring from one node of the network to another. If a node determines that the message is not intended for that particular node, then it will pass the message on to the next node of the ring. The problem is that every node on the ring could read or intercept data intended for another node, allowing for the potential compromise of all data on the network.

ATM uses cell-relay technology. A cell is a fixed-size, fixed-format packet. Cell and Frame Relay technologies are protocols that break up a message into many packets and transmit each packet according to the most efficient route. Packets from the same message might have totally separate routes, and it is the responsibility of the receiving node to reassemble all packets into the original message. These packet-switched protocols allow for great redundancy and survivability. A significant portion of a packet-switching network must be disabled for communications to be lost. In spite of some inherent protection, ATM/SONET networks can be disrupted and data can be compromised. Indications are that early commercial and government implementations of ATM/SONET are not very secure.

ISDN is intended for high data transfer rates for low usage communications links. ISDN services are provided by the Regional Bell Operating Companies, and use local telephone lines. The protocol allows for two separate streams of data: a voice stream and a data stream. Separate data streams allow for simultaneous activities. Since ISDN services are dependent upon the PSN, they are susceptible to the same types of compromises that are faced by all other data transmitted over telephone lines.

2.5.1.4 Firewalls, Guards, and Multilevel Devices

Firewalls filter network traffic and prevent undesirable traffic from reaching protected computers. Firewall use is increasing and will continue to do so. The firewall technology can effectively secure networks from intrusion in many cases. However, different firewall vendors provide different levels of protection. Despite the potential for compromises, firewalls can provide one of the more effective protection mechanisms, when they are properly implemented.

Firewalls have several disadvantages. The firewall is a bottleneck for network traffic and a single point of failure for the local network. If a firewall does not function, all connectivity may be lost. Additionally, firewalls are not very versatile when it comes to providing additional services, such as allowing for new communications protocols. Effective firewalls also limit services to individuals, limiting system functionality and frequently limiting usability. Many organizations struggle with the security versus usability conflict.

Guards are processors that limit the exchange of information between systems. They generally operate on strict formatting rules and provide an effective means of segregating messages with differing classifications.

Multilevel devices are trusted systems or equipment which process information with differing classifications or categories and which permit simultaneous access by users with different security clearances while denying access to users who lack authorization. These devices, sometimes referred to as Multilevel Security (MLS), are being fielded within portions of DoD.

While all of these devices provide some measure of information security, there are few standards to guide systems administrators and users in the selection of products to ensure a uniform level of security for selected domains.

2.5.2 Electronic Battlefield

The proliferation of information is also heading to the battlefield. All U.S. military units rely upon information technologies for basic functionality. For example, the Global Positioning System (GPS) has improved the efficiency of military operations and weapons employment.

Not only are forces in the field better informed, they are also better equipped. The miniaturization of technology provides forces with portable computers and communications systems, allowing for the modification of plans, tactics, and strategies in real time.

New problems of compromise arise as portable technology is integrated into the battlefield. Additionally, equipment and technology are placed closer to the conflict, which could provide access to U.S. communications circuits, and thus to critical strategic and tactical information. Two separate methods of minimizing the ill effects of enemy capture should be considered:

authentication mechanisms and tamperproof containers or destruction mechanisms. Authentication mechanisms that minimize exploitation of captured equipment must be considered.

The electronic battlefield will create new training challenges. Our forces must be trained to operate efficiently both with and without new technology. They must be able to utilize fully the information provided by technology, but they must also continue to operate if their equipment is rendered useless. Training must not ignore basic skills, even when the environment relies upon technology.

The following extracts from Special Report: Bosnia, The Role of I.T. in Operation Joint Endeavor, a Supplement to Federal Computer Week, April 29, 1996, [FCW] illustrate some of these points:

- While information technology can't move mountains or dry up mud, units in Bosnia have proven that sophisticated systems can surmount the formidable problems posed by both.
- The Army extended voice, data, and video networks down to infantry company users at forward operating bases.
- Military forces from more than 30 nations are participating in Joint Endeavor, and they must all be tied into the unclassified network.
- British, French and U.S. tactical systems have been integrated into one cohesive network, with even the Russian brigade tied into the U.S. tactical satellite network.
- The Army overcame significant technical challenges to provide Internet service over the narrow-bandwidth tactical command and control networks.
- NATO has also purchased more than 200 suitcase-type tactical satellite terminals for use by top commanders in the theater.
- The wide-band network was installed as part of the DISA/DARPA $88 million Bosnia C2 Augmentation (BC2A) Network. Besides providing much-needed wide-band connectivity, BC2A also includes the first operational deployment (for military purposes) of a Global Broadcast System (GBS).
- The V Corps video teleconference system runs over tactical links, while an intelligence community VTC system runs over the Defense Information Systems Network circuits, allowing face-to-face conversations not only with personnel in the European theater but all the way back to the Pentagon.
- The Joint Endeavor telemedicine network will use high-bandwidth circuits—up to 4 megabit/sec—to support such applications as telesurgery, telemedicine, telepsychology, and teledentistry. The Army wants to use telemedicine to bring specialists to the patient rather than the other way around. Weather conditions in the region also served as an impetus for the telemedicine network.
- The Joint Total Asset Visibility (JTAV) system tracks assets whether they are on order from a supplier, in transit, or in storage.
- Most U.S. units in Bosnia, Croatia, or Hungary—whether housed in tents, trailers, or shot-up office buildings—are equipped with several commercial off-the-shelf computers and workstations.
- Many information technology vendors have followed their products into Bosnia, providing support and maintenance.

- In Operation Joint Endeavor, the military is relying on new imagery software and other off-the-shelf technology to deliver 3-D and multi-layered maps to the field.
- Since Operation Joint Endeavor began in December, the Defense Department's combat photo journalists have dispatched thousands of images from the field in digital format.

2.5.3 Emerging Technologies

As a part of its Joint Warfare Capability Assessment of Information Warfare, the Joint Staff (J6K) requested the Institute for Defense Analyses (IDA) to research, analyze, and evaluate open systems technologies within the DoD and private industry to baseline IW technology. The results of that effort are outlined in a document [IDA 1] and a paper [IDA 2]. These are available from the Joint Staff (J6K).

The IDA Document identifies 56 technologies with potential information warfare application and, for each technology, describes the technology strengths and weaknesses, possible concepts of operation, potential risks and related information such as technology availability, points of contact, and patent or proprietary aspects. Table 2-5-1 shows the technologies. The Joint Staff specified the technology grouping (concepts, device technologies, software, and system integration). The Joint Staff also designated the three system-oriented activity categories with the following brief definitions:

- Nodes are discrete functional elements that include sensors, facilities for data and information storage and processing, and automated devices for presentation, analysis, and decision making.
- Links are networks and communications for linking nodes to transmit unprocessed and processed sensor data, and to collect and disseminate information such as status/situation reports, archival data, and intelligence, and command messages or task assignments.
- Human Factors designate the visual, aural, and tactile interfaces between automated equipment/machines and human operators/analysts/decisionmakers.

Table 2-5-1. Information Warfare Technology Matrix

TECHNOLOGIES	Activity Categories		
	Links	Nodes	Human Factors
Concepts			
Immunological approach to change detection			x
Visualization of computer operations (algorithm animation)			x
Computing with DNA molecules			x
Stereo image processing			x
Natural evolution of machine codes: digital organisms			x
Semiotics			x
Mediology			x
Direct link from the brain to a computer	x		x
Computational sociology (social organization across extended networks)	x		x
Device Technologies			
Fiber-optic undersea information network		x	
Microelectromechanical sensors	x		
Multiplexed communications with femtosecond laser pulses	x		
Electrooptical data storage on thin-film photoconductive materials		x	
Three-dimensional holographic storage of digital information		x	
Passive millimeter-wave camera		x	
Cesium vapor optical correlator		x	
Blue-green diode lasers	x	x	
Gallium nitride blue and ultraviolet laser diodes	x	x	
Protein-based computers		x	
Optical flux-monitoring molecular beam epitaxy control system	x	x	
Quantum electronic computer device technology		x	
Modulable retroreflectors for coherent CO_2 laser communication	x		
Holographic visor displays		x	x
Integrated neural network for image detection and classification		x	
Software			
Real-time video insertion	x		x
Fractal information storage	x	x	
Speech recognition technology for hand-held computers			x
Distributed execution environment for high-performance parallel processing	x	x	
Image deblurring		x	
Multispectral imagery analysis		x	
Speech recognition for Windows-equipped personal computers			x
Soft-copy mapping system	x	x	x
Neural networks and fuzzy logic		x	x
Security architectures	x	x	
Distributed operating systems	x	x	
Distributed multimedia processing	x	x	x
Agent-oriented software/distributed artificial intelligence	x	x	x
Network intrusion detection	x	x	
Collaborative information sharing on the World Wide Web	x	x	x
Wavelet-based image compression	x	x	

Table 2-5-1. Information Warfare Technology Matrix (Continued)

TECHNOLOGIES	Activity Categories		
	Links	Nodes	Human Factors
System Integration			
Three-dimensional command-and-control information display		x	x
Synchronous optical network	x		
Wearable computer systems			x
3-D micro-imaging and visualization		x	x
High-performance multicomputer for 3-D graphics		x	x
Ultra-high-performance multicomputer for 3-D graphic		x	x
Haptic displays (force feedback for virtual environments)		x	x
Nanomanipulator		x	x
Optoelectronic head-tracker for head-mounted displays			x
Ultrasound visualization (augmented-reality echography display)		x	x
Electronic support measurement bistatic sensor technology		x	
Acoustic daylight ocean noise imaging system		x	
Laser beam propagation through atmospheric turbulence	x		
Integrated optical-digital correlation		x	
Real-time 3-D imaging and control		x	x
Directed search testbed and collaborative analysis and decision-making		x	x

The companion IDA Paper identifies a subset of the 56 technologies which were subjected to a closer examination for potential payoffs, feasibility, and risks. Twelve information technology application areas were identified for priority consideration. For each area, the Paper describes the technology or technological area and its applications, summarizes the potential payoff from exploitation of the technology, identifies the elements of risk and potential risk mitigation factors, and suggests programmatic approaches to exploiting the technology. Table 2-5-2 lists the technology applications for priority consideration.

Table 2-5-2. Technology Applications for Priority Consideration

- Advanced Computational Concepts
- Framework for Development of Tools for Offensive IW and C4I Performance Enhancement
- Image Representation
- Diode Laser Applications
- Interfaces for Enhanced Situational Awareness
- Automatic Target Recognition
- Foliage Penetration Technologies
- Passive Polystatic Surveillance Networks
- Laser Communications for Video Transmissions
- Microsystems as Electronic Sensors
- Microwave Emitters

In 1995, the Defense Advanced Research Projects Agency's Information Science and Technology (ISAT) office commissioned a Summer Study on Survivable Distributed Information Systems. The purpose of the study was to determine whether the nation's critical information infrastructure could be hardened to improve survivability against a wide range of possible intentional and accidental threats. The study found the following:

- The systems that matter are often complex and unstructured with multiple legacy and commercial off-the-shelf components.
- The process of hardening complex systems is poorly understood.
- Laboratory successes are not impacting the nationally critical technologies.
- There is a requirement for a practical technology for selectively hardening complex systems to achieve high confidence solutions.

The study suggests a concept of wrappers to satisfy this requirement. The concept allows the superimposition of a framework with a well specified structure, captures the critical elements of the underlying system, and offers a form of leverage with which to introduce robustness solutions. The wrapper concept suggests intercepting the Input/Output of existing components, applications, and data to provide additional capabilities for fault tolerance, security, intrusion detection, system reconfiguration and systems management.

The study also analyzed two infrastructures, the electric power distribution and financial services. The study analyzed the vulnerability of the infrastructures to information warfare and recommended improvements to the robustness of the infrastructures. Tables 2-5-3 and 2-5-4 summarize these recommendations.

Table 2-5-3. ISAT 1995 IW-D Summer Study Recommendations on Electric Power Distribution

- Protect all Control/Monitoring/Communication Sessions in the Region.
    - Encryption, Authentication, Authorization.
    - Effortless Admin, Call Setup.
- Make Good Firewalls and Testers.
    - Vulnerability Evaluation Tools.
- Develop Simulations.
    - Operator Training.
    - Red Teaming.
    - Disaster/Attack Recovery.
- Develop Aids for Intrusion Detection.

Table 2-5-4. ISAT 1995 IW-D Summer Study Recommendations on Financial Services

- Strengthen End-System Robustness.
  - Multi-function Smart Cards with Cryptographic Services.
  - Selective Cryptographic Functions.
  - Real-time Fault-tolerant Operating Systems.
  - “Anticipatory” System Behavioral Monitors.
  - Computational Service “User Agreements.”
- Strengthen Networking Robustness.
  - High Bandwidth Circuits.
  - Authenticated, Encrypted Virtual Circuits.
  - Bandwidth Reservations.
  - Network “User Agreements.”
  - Selective Partitioning & Routing.
  - Certification Authority Structure.

2.5.4 Research and Development

In the area of defensive information warfare research and development, the Defense Advanced Research Projects Agency (DARPA), the Defense Information Systems Agency (DISA), and the National Security Agency (NSA) have signed a Memorandum of Agreement to cooperate in the development of new security tools and applications. DARPA supplies its ability to apply high-risk R&D to solve complex problems requiring advanced technology and support state-of-the-art feasibility demonstrations using leading edge technology. NSA supplies expertise in cryptology development and encryption, along with experience in conducting vulnerability analysis for the intelligence community. DISA provides the test beds for inserting these new technologies into information systems operations in a scaleable, modular fashion and will support the transition of the prototypes into production systems that can support the entire Defense Information Infrastructure. Tables 2-5-5 and 2-5-6 show DARPA and NSA technology research areas. [IDA 1]

Table 2-5-5. DARPA Technology Research Areas

- Artificial Neural Networks.
- Broadband Information Technology.
- Defense Information Enterprise (Scalability).
- Defense Technology Integration and Infrastructure.
- Education and Training.
- Information Survivability.
- Intelligent Systems.
- Microsystems.

Table 2-5-6. NSA Technology Research Areas

- Trusted Operating Systems.
- Firewalls.
- Network Countermeasures.
- Security Management.
- High-Speed Encryption.
- Biometrics.
- Cryptography.
- Secure Data Bases.

This page intentionally left blank.

2.6 INTELLIGENCE ENVIRONMENT

WHAT'S NEW?

This section has been enhanced to include material on threat goals and techniques, as well as information on current intelligence community information warfare activities. Other sections have also been updated to encompass current developments.

2.6.1 Introduction

Information warfare has both offensive and defensive aspects. Adversary issues play a part on both sides of the information warfare equation. In order to mount an effective offense, the adversary must be understood in sufficient detail. This entails "knowing thy enemy" in terms Sun Tzu would appreciate, i.e., knowing the infrastructure and decision process in detail. IW-D requires not only some knowledge about potential enemy information warfare capabilities, but also detailed understanding of one's own infrastructure and vulnerabilities. This clearly implies knowing more about the infrastructure and its interconnectivity, both here and abroad. But it also implies an understanding of the potential for new threats, to include the range of potential attackers, the types of attack, and the myriad targets that can be attacked.

Some new fundamentals apply to this warfare area. Much of the system architecture we might use in a war might be shared...some may even be shared with an adversary. It must be expected that any information system that is not totally closed from the outside world is vulnerable to compromise. Intruders have been able to crack many defensive technologies that have been developed, and it must be expected that they may compromise any new technologies that will be developed. In such an environment, rapid detection and restoration may be critical. Intruders do not have to exploit the technology if they can bypass the technology through non-technical means, or if disruption is the goal rather than exploitation. Many of the information warfare issues and questions are familiar, but the pace of change and scale of the problem is new. Moreover, the state-of-the-art in this technical area is in the commercial world—not in the DoD.

Information warfare attacks may not be made with the sole intent of disabling the military information infrastructure. The DoD operates within a larger national and international infrastructure of information systems. This infrastructure supports many functions within society, and those functions (not the supporting information infrastructure) may be the ultimate targets of information warfare actions. Thus, attacks may be aimed at disabling economic activities or safe air traffic control or power distribution in ways which constrain national or economic security. The defensive issues may be outside the purview of DoD, but are not beyond the scope of potential information warfare approaches to warfare and the concomitant requirement for information regarding adversary capabilities. Clearly, for DoD approaches to IW-D, knowledge of potential adversary functional capabilities must be collected and analyzed.

Information warfare creates comprehensive new challenges for the intelligence community. Offensive and defensive IW intelligence requirements are closely linked. Adversary capabilities and vulnerabilities are critical to both offensive and defensive operations. The traditional intelligence functions of early warning—detection; identification; mapping; and understanding the adversary, his thought processes, his perceptions, and his culture—must be reexamined. Coherent strategy, both in-depth and operational, for information warfare intelligence must be developed. This should not be simply a collection strategy; rather, it must also incorporate surveillance planning, data base and decision aid development, and considerations of timing and sequencing normally associated with operational planning. The strategy must address the following key issues.

The first challenge is the number and identities of potential adversaries. The United States faces a multipolar world, one in which it is much more difficult to determine who the next adversary might be and what his capabilities or vulnerabilities might be. The focus of the past 50 years on the former Soviet Union consumed a vast percentage of the intelligence resources, and at the same time lent some assurance to targeting. Today, there is a much longer list of potential adversaries, including non-state actors. A list of 20 or so possibilities adds measurably to the intelligence task, but does not capture the full spectrum of potential information warfare opponents.

The next step is to determine the adversary's current technological capabilities in the area of information systems and the actual information infrastructure. How this infrastructure interacts with others, with the international environment, and with the U.S. infrastructure is a central information objective. We must address ways to represent this infrastructure and its interconnections to the U.S. planners and commanders.

Technology proliferation is a particularly significant problem in information warfare, because the commercial world is driving the state of the art in many of the key technology areas. Another issue is that of understanding the adversary's potential future capabilities. The potential proliferation of information technology amplifies the list of potential adversaries and expands their capabilities. Understanding the dynamics of information and related technology proliferation is a crucial part of understanding the threat that potential adversaries might pose.

Yet another issue relates to understanding the opponent's decision processes, command and control processes, infrastructure, and sustainment functions. This issue involves knowing everything about the adversary, from who the decisionmaker is, to details about preconceptions, decision rules, data bases, and decision support systems, key advisors, etc. It is nearly impossible for the intelligence system to supply all of the necessary details, even when focused on a single or only a few adversaries. As an adversary's reliance on information and approach to its use may vary, this issue includes the way in which the adversary might plan to use his or her information system. Questions of emphasis, timing, sequencing, and network effects are only a few of the factors that must be considered.

One other point should be emphasized regarding information warfare. There is a potentially significant asymmetry in employable means between the adversary and the United States. A potential opponent can often use any means technically available to penetrate and exploit or disrupt and deny U.S. information systems—in peace as well as in war. The U.S. warfighters, however, may have significant constraints placed upon them by law and regulation, limiting their actions (see Sections 2.2 and 2.3 for an overview of the legal and regulatory environment).

These issues of adversary capabilities and potential capabilities, taken together, are the raw material of understanding how vulnerable an adversary might be to information warfare and how an adversary's capabilities may affect the United States. U.S. warfighters must include some sense of that vulnerability in planning; they must derive and further develop adequate measures of relative vulnerability. It is currently hard to model relationships of this sort, partly because adequate measures of effectiveness do not exist. Although some elements of information warfare can be measured in input terms, and some measures of merit partially described, there are still too many unquantified or unquantifiable terms (e.g., deception, perception management, command, etc.) to permit a detailed analysis. For example, a vulnerability that cannot be attacked (because appropriate systems do not yet exist, or other constraints apply) may not need to be immediately addressed. Such a judgment implies some sense of a net assessment against one's own capabilities—but it remains hard to attach numbers to such judgments.

For the defensive information warfare planner, the above considerations are also important. However, the focus shifts to assessing how potential adversaries perceive U.S. vulnerabilities, and how they might intend to exploit them. Although this might be a sufficient statement of the intelligence requirement, it entails many sub-elements of details, making it a very broad requirement indeed. Questions such as how much the potential opponent knows about the U.S. information infrastructure and decision process, what technologies the opponent might couple with what skills and what the opponent might know about U.S. perceptions, are only a few of these details. Furthermore, the key questions may not just focus on military capabilities and military doctrine. Information warfare by a potential opponent may have as its focus elements that go well beyond the Defense and military infrastructure. Targeting industrial or other targets is not new, but the information warfare manifestation may be particularly leveraged against non-DoD elements. This makes the information assurance task for the United States a very broad one, with potential for multiple government agency and civilian organization involvement. The comment regarding asymmetries applies yet again; the opponent may not have such a complex task of coordination.

Thus, the information warfare threat to the NII must be considered in developing future national security strategy. While an attack on the NII might not directly affect the capability of military hardware or warfighting capability, such an attack could surreptitiously (or visibly) cripple the United States without a shot being fired and without direct knowledge of who the adversary may be. For example, during Desert Storm, the allied forces concentrated fire power on the Iraqi NII. This left Iraq blind to attack, crippled the Iraqi economy, and demoralized the nation. While the allied forces primarily used munitions to destroy the NII, similar attacks may be accomplished against the United States through electronic means.

2.6.2 Intelligence Activities

The Report of the Commission on the Roles and Capabilities of the United States Intelligence Community (Brown/Aspin Commission), "Preparing for the 21st Century: An Appraisal of U.S.

Intelligence," issued on 1 March 1996, acknowledged the significance of the information warfare threat and the Intelligence Community's role in this important area:

"Collecting information about "information warfare" threats posed by other countries or by non-governmental groups to U.S. systems is, however, a legitimate mission for the intelligence Community. Indeed, it is a mission that has grown and will become increasingly important. It also is a mission which the Commission believes requires better definition. While a great deal of activity is apparent, it does not appear well coordinated or responsive to an overall strategy."[USC]

Although, according to some reports, the Intelligence Community came late to an awareness of the existence, nature, and scope of the IW threat, the Intelligence Community is now fully engaged. The Intelligence Community's information warfare activities are valid, timely and increasingly coordinated to maximize the derived benefit from many assets. Intelligence Community efforts in information warfare include the following:

- A National Intelligence Estimate on the information warfare threat to be issued by 1 December 1996.
- Creation of an Information Warfare Center of Excellence to be located at NSA and staffed with representatives from NSA, CIA, and DIA. It will focus on threats, vulnerabilities, and indications and warning.
- DIA, responsible for providing indications and warning of foreign military attacks against the United States and its interests, is leading a U.S. government-wide effort to ensure the challenges presented by information warfare are met fully by both the DoD and the National Indications and Warning Communities.
- A DIA-led U.S. government-wide effort, the Interdepartmental Information Warfare Threat Working Group, to develop relevant threat information.
- A DIA-led Information Warfare Working Group, to define a process and procedures for the coordination and production of threat assessments for information warfare-related activities.

Key efforts center around developing I&W capabilities for information warfare. The I&W problem is especially troublesome for several reasons. First, the intelligence sources necessary for I&W in the Information Age are significantly different from those used in traditional I&W (e.g., HUMINT and ELINT). The speed of information warfare attacks, coupled with near-anonymous offensive capabilities, makes it difficult to differentiate the nature and source of possible attacks. While information systems and network management tools (e.g., access logs, intrusion detection systems) offer possible sources for I&W, the government does not own or have complete access to these sources and does not have the authority to monitor them. This gives a potential adversary a backdoor into the infrastructure. Adversaries are most likely to penetrate the systems the intelligence community isn't watching and then launch attacks from the compromised system, further disguising their identity.

2.6.3 Adversary Capabilities

In today's multi-polar information-dependent world, the spectrum of possible U.S. adversaries has expanded to include, along with traditional nation state adversaries, non-state actors, rogue organizations and terrorists, and in the context of information assurance, perhaps even highly capable individuals.

Indeed, open literature originating in China provides detailed analysis of the strategic aspects of information warfare. A Chinese Army newspaper reports that:

"Owing to the increasing internationalization of information technology development and the integration of social, political and economic development, people now have to employ stealthier, more indirect and more "surplus" combat means when applying war means to resolve bilateral political contradictions. This means that along with the development of information technology and the constant perfection of information warfare, "visible" information wars are going to be reduced in scale so that it will be more difficult to predict when and where a "visible" information war will break out and what type of a threat a "visible information war will create." [CHINA]

Marketing materials from Russia offer a wide range of Electromagnetic Pulse (EMP) weaponry, from hand grenades to mortars. Printed advertisements show the weapons being utilized in several different environments, from office settings to commercial airports. Russian President Boris Yeltsin recently stated that, "While maintaining our nuclear potential at the proper level, we need to devote more attention to developing the entire range of means of information warfare ...." [YELTSIN]

At a lower level, hacker capabilities have maintained a constant threshold. The Rome Lab intrusions, detailed in a May 1996 GAO report, demonstrate that individual hacker intrusions still pose a threat to defense systems. As stated in the Air Force report on the incident, "We have only the intruders to thank for the fact that no lasting damage occurred. Had they decided, as a skilled attacker most certainly will, to bring down the network immediately after the initial intrusion, we would have been powerless to stop them." [GAO]

2.6.3.1 Threat Goals

A potential adversary could use information warfare techniques to achieve the following objectives or goals:

Unauthorized Disclosure of Data: Unauthorized disclosure of data implies unauthorized access to such information as sensitive security policy, foreign policy, intelligence information and operational plans. Access to this information provides an adversary advance warning of U.S. intentions and the ability to exercise countering moves such as diplomatic action, military deployments, strategic deception, third country tip-off, or political embarrassment. Unauthorized knowledge of U.S. plans, readiness posture, research and development initiatives, or program and requirement status could degrade the ability of the JCS, the Services, and the combatant commands to carry out their missions.

The location, capabilities, and readiness of deployed forces are of immense interest to an adversary. Should such data be compromised, an adversary may be able to determine command and subordinate vulnerabilities and details of strategic, operational, and tactical plans. With the multitude of platforms generating, transmitting, and receiving information via multiple C3 links, the possibility of compromise is great.

Corruption of Data: Corruption of data is an insidious method of deception which, if undetected, leads to faulty policy, procurement, and operational decisionmaking and execution. Once detected, the full extent of data corruption can be elusive, leading to service denial while the impact of the attack is determined and corrective measures are implemented. Corruption, once detected, calls into question the integrity of the system itself, as well as the data.

Spurious or altered information will impact any system that depends on information flows. At higher levels, corruption of data will tend to have broader impact. For example, tasking, mission assignments, and readiness information exchanged between CINCs and the NCA that is based on corrupted data will lead to flawed tasking and faulty advice. At command and service levels, corruption of data can lead to erroneous targeting, unit movements, and false, altered or deleted orders and logistics support. Loss of a planning system, for example, may require units to use slower, more labor intensive methods for development of air tasking orders or target registration for artillery. In fact, delays inherent in corruption or disruption strategies may be the primary objective of such information warfare approaches.

Denial of Service: Denial of service has serious consequences for operations, whether global in nature or in even mundane transactions. The technological success of U.S. forces in the Gulf War would not have been possible without the ability to exchange information in a timely fashion. Conversely, a key objective in the Gulf War was to deny C3 to Iraqi forces by directing a large portion of the air campaign against Iraqi C3 infrastructure. It is essential for the United States to protect technological superiority by the our ability to communicate and pass data on demand.

At the highest level, denial of service impacts the ability of the chain of command to support the NCA and exercise its prerogatives in providing direction to subordinate commanders. Loss of communications paths, C3 nodes, or network connectivity will result in loss of efficiency and effectiveness, particularly in crisis. The loss of telephone service (either secure or unclassified) can interrupt the most routine activities.

Disruption of Communications: The military theory of the former Soviet Union included strong incentives to disrupt an enemy's ability to communicate, as a prerequisite for, or in support of, operations. More recently, in the aftermath of the Gulf War, the Russian military theorists indicate that gaining an initial information advantage is potentially war winning. Losing the ability to communicate can leave a military unit in the dark, forcing every individual soldier and unit to operate independently of others. A coordinated attack becomes nearly impossible, particularly in a rapidly changing situation. Communications are vulnerable on many levels, and attacks on all levels of communications should be expected.

Communications also can be disrupted on a national level. Communications occurring between senior national or military leaders can be critical to the execution of military operations. There are several methods that can be employed to disrupt communications at this level. For example, adversaries might be able to damage satellite communications by disabling the satellite transmission stations, by disabling satellites themselves, or by jamming, intrusion or other soft-kill mechanisms.

The U.S. military relies heavily upon the use of commercial telecommunications for all levels of communication. As will be discussed later, there are many threats to telephone lines, both nationally and internationally. A disruption in the telephone system could cause a loss of communications.

Radio transmission is a central element of military communications and may be disrupted in many ways. While large-scale jamming and disruption are not usually feasible, selective jamming is possible at critical points in operations. Additionally, attacks on stationary transmitters and relay stations should be expected from a variety of conventional and non-conventional sources. Although this is not new, some of the potential attacks may have a different character in the rapidly changing environment of global communications. There are a number of new techniques, or old techniques with new applications, which expand the spectrum of threats to communications systems.

2.6.3.2 Threat Techniques

Threat techniques and tools, particularly used with intent, take on many forms. Some may be easy to identify and even to detect but are difficult to counter. Others may not even be detectable. Still others may be put into place and not activated until some later, more opportune time. There must be heightened sensitivity to such activities, as the DoD uses more foreign-based COTS components. Examples include:

Masquerading — An attempt to gain access to a system by posing as an authorized user. Once this access is achieved, sensitive and classified data can be compromised and services stolen.

Spoofing — Insertion of extraneous data or comments in an effort to cause a system to inadvertently disclose information or data.

EW — Electronic Warfare is made up of three components: Electronic Attack, Electronic Warfare Support, and Electronic Protection. As a threat, EW can cause denial of service and corruption of data by employing electromagnetic energy at any point in the spectrum. For example, jamming can inhibit or obstruct the transfer of information; electromagnetic pulses can corrupt data stored on magnetic media and damage software and hardware.

SIGINT — An orchestrated signals intelligence-based threat serves multiple purposes. Not only can SIGINT provide the basis of information to apply other threat means, it can also provide insight into data sensitivity levels, communications and information structures, and transfer schedules and data loading.

Intrusion — Surreptitious attack by such entities as hackers, disgruntled employees, and foreign intelligence agents are increasing in frequency and have potential impact on information processing, storage, retrieval, and transfer assets. The impact of malicious codes such as viruses, logic bombs, trapdoors, Trojan horses, and time/even activated software, applications, and/or firmware is well documented. Cautionary procedures must be used when integrating AIS components procured from foreign vendors or governments. Additionally, data base misinformation represents a relatively new dimension to data tampering; the effects may not be detectable for long periods of time and may affect not only the systems entered but all systems that share information with it.

Substitution and Modification — An intruder can disrupt decisionmaking, planning, and operations by modifying or substituting false data or information in a U.S. system. The objective can be to impact a specific decision, plan, or operation or, in general, to shake U.S. decisionmakers', planners', or operators' faith in the integrity of information available to them.

Directed Energy — Although many of the technologies associated with directed energy (i.e., lasers, particle beams, high-powered microwaves) weapons and techniques are not mature, there is still cause for concern for our information infrastructure. Capable directed energy methods, when directed at information processing and transfer assets, can cause corruption of data and denial of service through destruction or degradation of hardware, software, or firmware.

Physical Destruction — Hostile acts of adversary forces, terrorists, or destruction as a result of natural disaster can be the most devastating form of threat to information processing and transfer resources. Not only can facilities and resources be lost, but the potential loss of stored data or key information transport nodes—connectivity—can be far more devastating.

Unauthorized Access — Access to information processing and transfer resources by unauthorized persons presumes, in many cases, that the threat is internal to the organization. Typically, some knowledge of an organization's systems, procedures, and security barriers (either physical or logical) is required. In the past, however, states have demonstrated skillful human intelligence capabilities by infiltrating select government positions. In the Information Age, states may target key positions that provide physical access to sensitive and classified information systems.

Cover and Deception (C&D) and Psychological Operations (PSYOP) — In the military environment, C&D and PSYOP have been used throughout history. U.S. adversaries, from North Vietnam to Somalia, have used information to influence U.S. policy and public opinion. In the past, the United States and its adversaries have used various techniques to influence military operations.

C&D and PSYOP have also been used to demoralize an enemy or to sway public opinion against military actions or government decisions. In many cases, effective use of C&D and PSYOP has proved to be a more powerful weapon than military actions. Defense against such an attack is difficult.

Good intelligence data can alleviate the threat posed by C&D. Nevertheless, C&D use can increase uncertainty in a commander's decisions. Uncertainty implies delay, and delay can be critical to military outcomes.

PSYOP are even harder to control. Widespread dissemination by the U.S. media and its independence of military control vastly complicate military operations. Any information warfare strategy must take into account the press and at least address its potential impact. It will be a key component of the information environment.

2.6.4 Threats to the Information Infrastructure

There is a significant threat posed by adversaries of the United States Government to U.S. information assets throughout the world. It is generally accepted that if a single person has developed the capability to compromise an information system, then any group or individual may obtain the knowledge or services of that person. Thus, the potential threat of software or hardware attacks on computer systems must be carefully evaluated as a part of any information warfare strategy. The potential adversaries include countries and other groups (and individuals) which seem likely to have hacker-like capabilities. While traditional computer hackers do not necessarily represent a direct threat from an information warfare perspective, they provide the knowledge for U.S. adversaries to wage devastating attacks against a variety of assets. Usually, hackers are the first group of people to become aware of U.S. vulnerabilities, and unfortunately, they can share their knowledge with anyone.

2.6.4.1 Who is the Adversary?

Hundreds of traditional and non-traditional groups of people could be considered potential adversaries. As noted above, the cast of possibilities has been expanded in the current, multilateral environment, and detecting and tracing such activity can be very difficult. The Department of Energy and NSA estimate that more than 120 countries have established computer attack capabilities. [GAO] Determining the adversary is a major part of the challenge for information warfare.

Potential opponents are interested in compromising data on various types of information systems. It has been established that the KGB sponsored the Hannover Hackers, who gained illicit access to over two dozen computer systems that contained classified information (as well as many more which did not). The Hannover Hacker case is a rare case where state-sponsored espionage has been acknowledged. DISA reporting indicates that numerous intrusions continue, and the scale of the attacks may be increasing.

Nations that are considered to be friendly to the United States have also acknowledged espionage against the United States. In almost all of these cases, the stated goal of the espionage was economic intelligence. Countries have been accused of, and have admitted to, obtaining data from the U.S. Government and U.S. corporations through information warfare-related measures. While economic intelligence may not seem to be a direct threat to U.S. security, the losses suffered by the United States are measured in billions of dollars. Additionally, any stolen technologies are no longer controlled by U.S. export regulations, and are more easily available to U.S. military adversaries. Most important, the techniques used are equally applicable to disruptive purposes. Even if not targeted against the military directly, some attacks could be mounted to disrupt significant elements of the domestic economy and infrastructure (functional attacks, as noted above), which would delay or disrupt support to the military, cause damage to the United States, and potentially cause widespread secondary effects (financial loss, cutting power or services, etc.).

Other adversaries may be concerned with transferring sensitive technologies and identifying targets for terrorist attack. This category would also include organized crime, which is included in the theft of funds, money laundering, extortion, etc. This category of adversary might be either a foreign or a domestic threat. There are individuals and organizations within the United States that are capable of various levels of attack. While the media has publicized the threat from individuals, there are organized groups that may be similarly disposed to harming the U.S. infrastructure. Some groups reportedly have developed units that are knowledgeable in information warfare.

From an information warfare perspective, hostile countries and terrorist organizations represent the most significant threat to U.S. national security. While economic competitors may be inclined to compromise the data on information systems, they are not likely to mount denial-of-service attacks on the infrastructure. However, economic competitors are sponsoring research that can assist hostile entities.

2.6.4.2 The Extent of the Threat

U.S. adversaries are—or certainly will be—significantly able to compromise any information system in use by the U.S. Government that has any connectivity to the outside world. Information systems, as defined for this section, would include any system involved with computing or communications.

Skilled intruders have infiltrated the foundations of PSNs throughout the world. PSNs include telephone systems and cellular communications systems. Intruders have obtained the computer software that controls the telephone systems, and there is proof that they have modified the software to include hidden ways for them to obtain access to the telephone system if authorities seal the known ways into the system. Intruders have been known to monitor conversations, reroute calls, change telephone numbers, add new telephone numbers, etc.

In view of the routing of 95 percent of military communications over commercial telephone lines, such capabilities pose a substantial threat. While the communications may be encrypted, the threat of denial of service is severe. Crippling even a small portion of the PSN could substantially impact military communications.

Commercial users of these communications networks must also be considered. Many large organizations, including the world's largest banks, rely upon public networks to perform their day-to-day operations. Billions of dollars of commerce pass over these networks every day. Intruders have been acknowledged to have compromised them. There have been several reports of criminals penetrating such communications and stealing extremely large amounts of money from financial institutions. The networks in question also provide connectivity to the U.S. Federal Reserve.

Intruders who have stolen money from financial institutions have, in some cases, been sponsored by organized crime, terrorist organizations, and hostile governments. Foreign governments are creating hacker-like capabilities. For example, friendly governments are reportedly sponsoring research on computer intrusion. While these countries might not be interested in waging information warfare against the United States, the knowledge they gain might not be confined to the friendly government.

Currently, some intruders can compromise most known countermeasures. Attackers have been able to counter dial-back modems, virus detection mechanisms, one-time password methodologies, and some encryption devices. However, technologies and procedures are available to mitigate the threat.

If technical measures are unsuccessful, intruders and other entities may resort to non-technical measures. These non-technical measures can include methods that are traditionally associated with Human Intelligence. Hackers use the term Social Engineering to describe their Human Intelligence effort. Social Engineering may include calling random people at the targeted organization and asking them for their passwords or modem telephone numbers, or going through an organization's garbage to find any information that may compromise a computer system. Generally, a Social Engineering attack may be more efficient than a traditional Human Intelligence effort, because it is more narrowly focused, and it may be easier to keep the targets unaware of such attacks.

2.6.5 The Intelligence Challenge

Information warfare has been particularly troublesome for the Intelligence Community because IW is a non-traditional intelligence problem that is transnational in nature. It is also not easily discernible by traditional intelligence methods. Formerly, capabilities were derived from unique observables, indicators, sensors, pre-existing data bases, and classic analytic and training techniques. Likewise, intent was extracted from understood variables that offered measurable/actionable reaction time and graduated response options. With information warfare, however, the following elements come into play:

- Observables, indicators, experience, data bases and training associated with historic threats and their manifestations are rendered largely useless.
- Key technologies have completely innocent applications. For example, software used to test systems can also be used to penetrate systems.
- Significant capability can be purchased at low cost. Information warfare generates yields equal to or greater than those that can be obtained with the same resources using traditional military capabilities.
- Quantification (i.e., number of tanks, planes, etc.) is largely irrelevant.

Technology transfer further complicates the picture. An actor's capabilities are not dependent on indigenous technology or industrial base; "Quantum Leaps" in capability will be possible as information warfare technology is offered on the open market; and some opponents may have or acquire more advanced technology than the United States possesses.

The challenge to the Intelligence Community is to overcome the obstacles and limitations of historic viewpoints and methods, and while respecting legal considerations, find a way to identify information warfare threats and warn of impending attacks. Determining the extent to which information protection for national security coincides with prudent business practice in the coming age is the first step toward the collaboration that will be required of all participants in the future.

SECTION 3

ORGANIZATIONAL CONSIDERATIONS

WHAT'S NEW?

Findings and observations from the original report have been updated. On-line resources for additional information on the organizations reviewed have been added to the organizational summaries in Appendix A.

3.1 APPROACH

Figure 3-1-1 shows the types of organizations that have an information warfare role and those that have information warfare related missions and functions.

- ***International***
- ***National***
  - **Public**
    - **Academia**
    - **Public Interest Groups**
  - **Private**
    - **Industries**
    - **Associations**
    - **Alliances**
- ***Federal Government***
  - **Executive Branch**
    - **Department of Defense**
    - **Other Departments**
    - **Interagency Groups**
    - **Advisory Committees**
  - **Independent Establishments and Government Corporations**
  - **Legislative Branch**
  - **Judicial Branch**
- ***State and Local Governments***

Figure 3-1-1. Organization Types Considered for Review

The basic approach to determining what organizational considerations might influence the development of information warfare policy and strategy included two key initial steps. The first was to identify organizations within DoD that were currently involved in information warfare activities. The second was to identify the various stakeholders in the development of the information infrastructure. This second step uncovered a very extensive and diverse set of organizations for which information warfare responsibilities are suggested, but not necessarily clearly defined. The Joint Staff Information Warfare Division (J6K) decided to focus most of the task efforts on this second set of organizations since the environmental considerations, previously addressed, appear to be more closely related to this second set of organizations.

3.2 SCOPE

Figure 3-2-1 shows the relative number of organizations in each category (indicated by the width of the rectangles) and the relative complexity of organizational information warfare issues (indicated by the height of the rectangles). It was not possible to identify completely all of the organizations which have information warfare related missions and functions, let alone visit all the identified organizations or investigate all relevant issues. The shaded rectangles represent the coverage of differing organizations in this report.

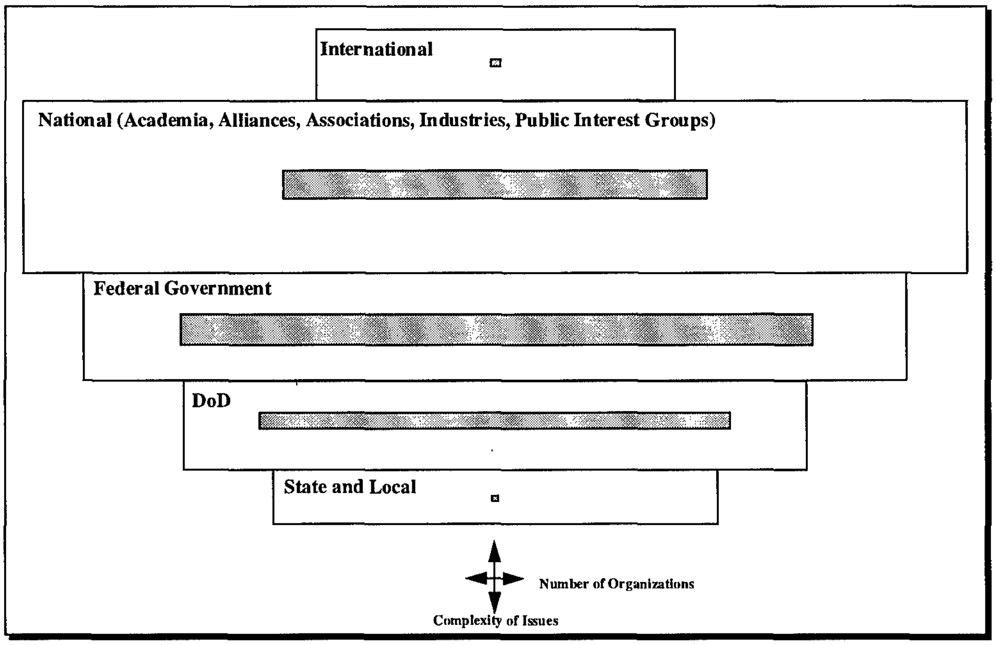


Figure 3-2-1. Scope of Organizations and Organizational Issues Addressed in Report

Based on the intended focus and scope of this report, international and state and local organizations were not reviewed. The number of these organizations and the complexity of related issues is, in fact, quite extensive. Example organizations and interests include the United Nations (coalition information warfare partners), International Telecommunications Union (international telecommunications standards, international frequency spectrum allocation), General Agreement on Trade and Tariffs (export and import controls), INTELSAT (use of international satellite communications resources), state public utilities commissions (regulation of telecommunications service providers within state boundaries), and county and city governments (regulation of cable television franchises). A review of these organizations and issues may be made in the future.

3.3 REVIEW

The review encompassed researching documents and on-line resources, visiting over 100 organizations, and interviewing personnel. More than half of the reviews involved visiting the organizations and interviewing key individuals in those organizations. Those organizations reviewed are identified at the index to Appendix A, Organizations and Activities. Appendix A also includes, for each organization reviewed:

- An organizational chart.
- An organizational summary which identifies
  - A senior information warfare/information assurance official.
  - Key points of contact.
  - On-line resources for additional information on the organization.
  - Information warfare/information assurance-related missions and functions.
  - Information warfare/information assurance activities, issues, best practices, and lessons learned.

3.4 FINDINGS AND OBSERVATIONS

Over the past year, it would be reasonable to summarize that although virtually none of the major issues, concerns, and deficiencies associated with national IW implementation have been completely resolved, the trends are positive; in some cases, markedly so. Given the breadth and complexity of this undertaking, it would be unreasonable to expect more rapid progress. In some cases, for instance national infrastructure vulnerability, more sophisticated attention to the issue has the initial/immediate effect of making the "problem" side of the equation seem to grow. This rigorous and serious attention, however, is judged to be a necessary first step toward the objective and comprehensive treatment of such complex and pervasive issues. Thus, we see that some problems remain:

- Within the Federal government and the private sector, **there is still no set of universally agreed-upon terms and definitions** to permit a common framework to discuss information warfare and information assurance issues and how they might be resolved. Figure 3-4-1 illustrates some of the terms used in DoD, in other departments of the Executive Branch, and in industry. While there has been visible progress in developing terms of reference within the Department of Defense and among the engaged segments of the "National Security Community" in defense, law enforcement, and the private sector during the past year, we will eventually require complete, consensus-based agreement by all segments on the terms and definitions needed for comprehensive policy treatment of this dynamic issue. The recent work of the Critical Infrastructures Working Group and the establishment of a Presidential Commission on Critical Infrastructure Protection will aid considerably in developing the needed terms and definitions, particularly since the Commission will include active participation of the private sector. A glossary has been added to Appendix B of this edition of the report to aid in understanding of the terms. The glossary is not meant to be authoritative.

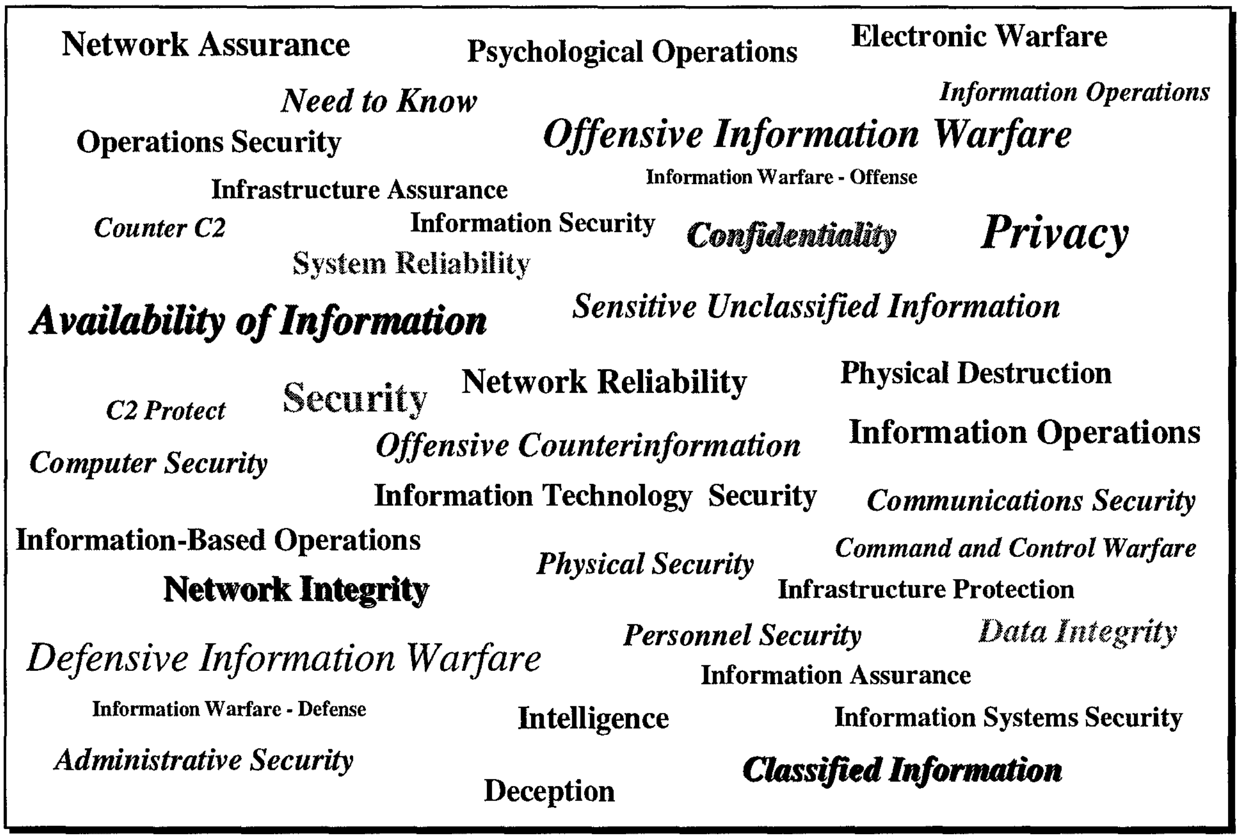


Figure 3-4-1. Some Information Warfare Terms in Current Use

- **Dependency on and influence of vulnerable infrastructures is not well understood.** Understanding of the dependency of critical security and economic functions on the national infrastructures has grown considerably in the past year. Rigorous understanding by functional proponents of the dependencies on infrastructures and the vulnerabilities of those infrastructures is lagging at present.

  However, coverage of security issues by the regular and trade press, military initiatives, and new awareness activities by the Federal departments and agencies have all served to increase the breadth and depth of understanding of the information infrastructure vulnerabilities. A few organizations are also beginning to analyze the infrastructures. While the focus and approach of each analysis identified vary considerably and the efforts have to date not been well coordinated, the efforts do begin to illuminate the issue and thereby demonstrate an increasing awareness of the functional dependencies and the infrastructure vulnerabilities. The Joint Staff recently completed a draft Mission Need Statement on Infrastructure Assurance Modeling And Analysis. When implemented, this capability will aid substantially in determining the impact of infrastructure dependence and infrastructure vulnerabilities on military deployments and operations.

The Department of Defense and the Federal government are not sizable market forces, and therefore, they are not capable of solely or significantly influencing the assurance of the national infrastructures on a purely economic basis. Both entities can increase their influence by being better informed, more knowledgeable, and demanding customers. However, it may be necessary in some cases for both to propose law, regulation, or policy necessary for assurance or pay for added assurance as a part of contracting for services.

- **The perceptions of information warfare issues are based on individual experiences and organizational missions and functions.** From the experience perspective, the Computer Security Act of 1987 resulted in a clear division of responsibility between the DoD and the DoC regarding the protection of classified and sensitive unclassified information. The extensive and vigorous debate preceding the legislation created a lasting impression on the participants, many of whom are now senior managers responsible for the continued implementation of the provisions of the Act. The Clipper chip proposal has solidified in the minds of industry and civil libertarians the view that the Federal government might attempt unwarranted intrusions. And the recent establishment of the U.S. Security Policy Board has met with some resistance; some members of agencies of the Federal government perceive that the Board may infringe on their responsibility for developing, promulgating, and implementing sensitive but unclassified information guidelines and standards.

  From an organizational perspective, the law enforcement, defense, market, and intelligence communities all have significant interest in electronic intrusions and other information warfare related matters. However, because of their different missions and functions, the individual communities' perceptions of the issues may be significantly different. For example, the law enforcement community would probably view an electronic intrusion into a financial network as an attempt to defraud and would be intent on gathering evidence to prosecute the intruder. The defense community might view it in several ways: as a diversionary effort to aid in concealing a more significant intrusion into its command and control structure; as possible evidence of an information warfare attack on the United States; or as possible means to obtain funds to purchase proscribed weapons of mass destruction. The market community might view the intrusion as an act of economic espionage and request the assistance of the counter-espionage arm of the FBI, which might have competing interests vis-à-vis the rest of the law enforcement community. And, finally, the intelligence community might view the intrusion as an opportunity to gain intelligence about the intruder.

  The perception of issues based on individual experience and organizational missions and functions may initially inhibit meaningful discussions of infrastructure assurance policy issues but should be mitigated by increasing dialog on these issues.

- **Responsibilities for information protection are not consistently assigned within the Executive Branch departments.** In some departments, all security and protection responsibilities (information, document, communications, personnel, administrative, physical, etc.) are centralized in a security organization. In other departments, some of the responsibilities are centralized in the Information Resources Management organization. In still other departments, the responsibilities are split among several organizational elements. With the growing attention to infrastructure protection and assurance, additional organizational elements, such as those responsible for emergency planning and continuity of operations, should be included in policy formulation. It is possible, however, that the recent creation of Chief Information Officer positions in the Federal departments and agencies as mandated by the Information Technology Management Reform Act will result in the streamlining of these responsibilities.

- **With the exception of the telecommunications infrastructure, there are no organizational structures and processes to facilitate the sharing of sensitive information needed for infrastructure assurance.** Needed sensitive information includes threat and vulnerability information, risk analysis and mitigation information, indications and warning (strategic intelligence), tactical warnings, and attack assessments. The NSTAC/NCS NSIE organizational structure and process for the telecommunications infrastructure serve as a possible model for the sharing sensitive information in other infrastructures. The recent focus on critical infrastructure protection has increased awareness of the need for sharing sensitive information in infrastructures other than telecommunications and will probably result in the creation of the needed structures and processes.

- In terms of information warfare-related capabilities, most organizations have historically focused on protection activities, and the investment strategies for the future are similarly focused. A limited number of organizations are developing capabilities to detect electronic intrusions and other disruptions. **Very few of the organizations have developed a capability to identify the nature of disruptions or intrusions (assuming they are detected), to restore the infrastructure in the event of malevolent disruptions, or to adequately respond to the information warfare attacks.** There are, however, a number of efforts under way to improve near-real-time detection and reporting of network intrusions. (See DARPA and DoE National Laboratories organizational summaries.)

- **In many organizations, budgets and staff to address information assurance-related matters are very limited.** Within the civil departments and agencies, staffs to deal with these matters are on the order of units, tens, and scores of people. Budgets for these same departments are on the order of units and tens of millions of dollars. As might be expected, everyone agrees that budgets and staffs are much too small. As a matter of fact, most staffs and budgets are diminishing, particularly throughout the Federal government.

- **All organizations reviewed are faced with constant change.** Government is reinventing itself. In some cases, Executive Branch departments are being considered for elimination. In other cases, departments will be reduced in size in the next 2 to 5 years. The deregulation of additional industries (e.g., electrical power generation and distribution) and increased competition have forced government and industry to rely more and more on information technology and to economize and centralize operations. Telecommunications legislation and regulatory reform will bring about the convergence of industries such as telecommunications, cable TV, and publishing. Companies are constantly trying to adjust their work force size, form the right alliances for competitive advantage, and acquire and merge with competitors.

Mergers and acquisitions in the private sector have increased dramatically in the past year with the result of producing more change, reliance on information technology, and economizing of operations. New technology is being introduced at an ever-increasing rate. In the face of this constant change, information assurance is the stepchild of operational and fiscal crises.

All that notwithstanding, we also find that:

- **Executive-level understanding of information warfare issues is growing.** Increased press and trade publication coverage of these issues during the past year have helped to increase the level of understanding. In some departments, those responsible for information security are demonstrating for senior executives the vulnerabilities of their information and information systems. Interest in infrastructure protection has, in fact, originated at the very highest levels of the Federal government.

- **Coordination of individual and collective agency efforts is becoming more focused.** The signing of PDD 39 and the creation of the Critical Infrastructures Working Group in late 1995 has served to focus the effort and enhance coordination. The proposed creation of a Presidential Commission on Critical Infrastructure Protection to study the issues and the creation of an Infrastructure Protection Task Force to provide an interim response capability to intrusions and possible attacks will aid considerably in defining the issues, providing direction, and coordinating the ongoing activities.

- **There is growing Congressional interest in information infrastructure protection.** The Kyl Amendment to the Fiscal Year 1996 Defense Authorization Act emphasized to the administration that the Congress views information infrastructure protection as a very serious matter. The Kyl Amendment directed the administration to provide a report on the "national policy and architecture governing the plans for establishing procedures, capabilities, systems, and processes necessary to perform indications, warning, and assessment functions regarding strategic attacks by foreign nations, groups, or individuals, or any other entity against the national information infrastructure." The House recently passed HR3230, the National Defense Authorization Act for Fiscal Year 1997 which also includes language calling for a similar report and directs the investment of specified percentages of the Defense Information Infrastructure budget in infrastructure security exclusive of NSA and DARPA investments in INFOSEC. Finally, the Senate Permanent Subcommittee on Investigations recently initiated hearings on security in cyberspace. While all this interest may be a two-edged sword, it does illustrate the seriousness with which the issues are viewed.

- **Information infrastructure assurance issues are becoming more visible.** Regular press coverage of related issues has grown, probably 100 percent in the past year. Increase in trade press coverage has been much more dramatic, probably over a 500 percent increase. Incidents such as the Rome Labs penetration and the Argentinean hacker have been front-page news. The series of "...the Day After" table-top exercises sponsored by the OASD(C3I) for senior managers and executives from throughout government and industry has aided significantly in awareness and understanding. The release of the recent GAO report [GAO] in conjunction with the start of Senate hearings has also added to the visibility of the issues.

- **Policy discussions are beginning to result in policy promulgation.** OMB published the Revised Appendix III to Circular A-130. The Joint Staff published CJCSI 3210.01, Joint Information Warfare Policy and CJCSI 6510.01A, Defensive Information Warfare Implementation. The Department of Defense has in draft a new directive on information warfare which will clarify responsibilities and direction. In some cases, formal promulgation of policy begins the process of developing suitable implementation practices. For example, there are several requirements for a risk-based management approach to the protection of information, but specific mechanisms and guidelines on how to implement the risk-based approach are just now starting to emerge.

- **The Military Departments of the Department of Defense have made numerous contributions to understanding of the issues and coordination of effort.** Most services have high-level working groups to institutionalize and implement information warfare concepts and initiatives. All services are intent on and succeeding in getting information, tools, and support to the operating forces. The three largest services all have established operational information warfare organizations and the USMC is supporting the operational units with billets. While each of the services seems to be developing its own taxonomy for information warfare consistent with its missions, traditions, and doctrine, the broad sharing among the services of information on their efforts has been beneficial. All of the services are using on-line surveys and other Red Team techniques to assess the state of their security posture. Most services are making an effort to integrate network and security management functions and to coordinate computer emergency response team activities. Several of the services have published new or revised information warfare policy documents within the last year. Service research and development efforts have been focused, in part, on emerging information warfare requirements.

- **Several Defense-wide information warfare efforts are of note.** An information warfare net assessment currently ongoing will provide insights into needed policy and organizational initiatives. Department-wide information warfare training activities have been reviewed by the DoD joint Inter-Service Training Review Organization Initiative for IW. The Naval War College has integrated information warfare play into its annual Global Games. While the standalone senior-level information warfare course it has taught for the past 2 years will not be continued, the National Defense University is in the process of integrating information operations courses into the required curriculum of each of its colleges. The Office of the Director of Defense Research and Engineering has developed a Joint Warfighting Science and Technology Plan which relates basic and advanced technology concepts development to information warfare functional requirements. DARPA and the NSA each have several research and development efforts under way to directly support information assurance activities. The U.S. European Command deployed an information warfare organization to Bosnia, the first-ever such operational deployment.

- **The Federal departments and agencies have also initiated numerous coordinating activities.** The Criminal Division of the Department of Justice has formed an Industry Information Center with government and industry participation which meets quarterly to share information on the law enforcement aspects of computer crime and network intrusions. The Federal Bureau of Investigation and the U.S. Secret Service have formed a coordination group to address computer crime issues. Several of the National Laboratories of the Department of Energy have extensive efforts under way to develop real-time intrusion detection and other security operations capabilities. The Department of Energy established an information assurance program. The Department of State has made security one of the foundations of its information infrastructure development. The National Institute of Standards will publish a set of Generally-Accepted Systems Security Practices in the summer of 1996.

While they are not new activities, it is important to note that NIST sponsors the Federal Computer Security Program Manager's Forum and the Computer Systems Security and Privacy Advisory Board. The Forum serves to coordinate Federal government activities related to the security of sensitive unclassified information and the Board, mandated by the Computer Security Act of 1987, provides a coordinating mechanism involving government and industry perspectives.

- **The Department of Defense, the civil agencies, and the private sector are creating more computer emergency/incident response capabilities.** This growing trend in emergency response was further substantiated with the release of revised OMB Circular A-130 which mandated the creation of emergency response resources within federal agencies. While some large agencies will create internal emergency response teams, many agencies will rely on externally available assets. NIST, for example, is currently creating a fee-for-service response capability (FedCIRT) which will be made available to federal agencies. Within DoD, emergency response teams at DISA and the AFIWC have been complimented with similar efforts by the Army and Navy. In the private sector, *Information Week* reports that "Faced with security threats that can shut down corporate computer systems and bring businesses to a halt, a growing number of organizations have formed internal SWAT teams to fight off hackers, thieves and computer viruses." [Violino] Membership in the Forum of Incident Response and Security Teams (FIRST) is expected to increase by 500 percent, from 50 members currently to 300 by the end of the year. There is also an increased effort to coordinate these emergency response efforts and create vulnerability data sharing processes to ensure that system administrators and response team members have current information on known, new and emerging vulnerabilities. DoD is leveraging from such commercial CERT^{SM} capabilities as Carnegie Mellon by participating in and sharing knowledge and insights where common interests intersect. Further information on specific emergency response teams as well as contact information can be found in Appendix A, Points of Contact.

- **Law enforcement cooperation provides a good operational model for reacting and responding to information infrastructure intrusions, disruptions, and attacks.** The capture of Kevin Mitnick, the notorious computer criminal, involved no less than 11 distinct public, private, and academic organizations at more that 20 locations. The Rome Lab and Argentinean Hacker investigations involved DoD, Federal, and international organizations. The Argentinean Hacker incident represented the first use of a Title III electronic surveillance of a computer system rather than a telephone or data line. Automated tools were used to identify the perpetrator as well as to ensure the privacy of innocent users of the system.

Study of lessons learned regarding the use of the laws, tools, processes, and procedures and the protection of privacy in these and other law enforcement incidents can certainly improve future cooperative efforts, both in the law enforcement and defense communities.

- **Intelligence support to infrastructure assurance is vital.** While the intelligence community is still grappling with the technical and analytical complexities of information age intelligence sources, collection, fusion, and dissemination, several important efforts have been initiated in the past year. Internally, progress has been made in areas of organization, resourcing, requirements/priorities, and mission focus. A National Intelligence Estimate is under way and is scheduled to be completed 1 December 1996. Several national-level working groups have been formed to develop information age indications and warning metrics, threats, and threat assessment processes.

SECTION 4

SUMMARY

The growing dependence of critical national security functions on vulnerable national infrastructures poses significant challenges to the Joint Staff, the DoD, the Federal government, and the Nation.

During the past year, there has been significant progress in awareness, understanding, coordination, and resolution of many of the challenges.

- **Awareness and understanding of infrastructure assurance issues have been enhanced** by coverage of security issues by the regular and trade press, conduct of table-top and other exercises, demonstration of information system vulnerabilities, and growing Congressional interest. Most importantly, interest in infrastructure protection has originated at the very highest levels of the Federal government.

- **Better coordination of the challenges is exemplified in several ways**. Several national-level working groups have been established to develop information age indications and warning metrics, threats, and threat assessment processes. Most of the Military Departments have established high-level working groups to institutionalize and implement information warfare concepts and initiatives. All the Military Departments are cooperating in the development of tools used to assess the security posture of systems and networks and in the development of training programs and materials. The Criminal Justice Division of the Department of Justice has formed an Industry Information Center with government and industry participation to share information on computer crime. The Critical Infrastructures Working Group was established in late 1995 and provided the first inter-agency activity to deal with information and infrastructure assurance issues.

- **Many of the challenges which existed one year ago are being resolved**. All the Military Services have established operational information warfare organizations or have provided information warfare billets to operational units. For the first time ever, an operational information warfare unit was deployed as a part of force deployment to Bosnia. Several new computer emergency/incident response organizations have been established. Defensive information warfare policy documents have been published by the Chairman of the Joint Chiefs of Staff and the Military Departments to aid in clarifying terms, definitions, and responsibilities. Joint IW doctrine is on a fast track and should be published in 1997.

While much has been accomplished in a very short time, many challenges remain. The following are highlighted because of their significance and complexity and because comprehensive solutions do not yet exist. The list is not all inclusive, nor should these challenges be considered necessarily the most important facing the community.

- **The dependency of critical national economic and security functions on domestic infrastructures is one of the significant challenges.** To begin, those functions that are critical are not necessarily well defined as such. For those that are, their dependency on portions of the infrastructure is not well understood. However, it is certain that in times of crisis and war, demand for information to support these functions will increase significantly and the supply of information (the capacity of the information infrastructure) will decrease, especially if the infrastructure is under attack. The information infrastructure is an extremely complex interconnection of numerous government, public, and private networks. More research is needed regarding the functional dependencies on the infrastructure, the vulnerabilities of the infrastructure, a risk management-based approach to protection, or the means and methods to restore and reconstitute in the event of a successful attack.

- **The evolution of the information infrastructure is influenced by a wide variety of stakeholders with complex, diverse, and sometimes competing interests.** The evolution requires a balance of the needs of the state versus the rights of the individual, the "Technology-Futurists" versus public sympathies and market forces, privacy versus law enforcement, and other confrontations. As with the resolution of all complex policy issues in a democracy, any policy initiatives seeking to influence the information infrastructure must take these stakeholders and their interests into account.

- **Near-real time management and control will be critical within the national security sphere in a crisis to minimize the impact and swift restoration of critical services.** Informal coordination and information sharing is on the increase; in a crisis, however, it is particularly important that roles and responsibilities be specified and rehearsed. While responsibilities are implied by existing policy, some ambiguity remains. Additionally, tools affording real-time management and control must be developed.

- **The Intelligence Community must overcome the obstacles and limitations of historic viewpoints and methods, and while respecting legal considerations, find a way to identify information warfare threats and warn of impending attacks.** Information warfare has been particularly challenging for the Intelligence Community because the classic threat equation becomes distorted. Traditionally, capabilities were derived from observables, indicators, sensors, pre-existing data bases, and classic analytic and training techniques. Likewise, intent was extracted from understood variables that offered measurable/actionable reaction time and graduated response options. With information warfare, however, observables, indicators and pre-existing data bases and training are less relevant.

- **The proliferation of new and emerging technologies complicates the information warfare equation.** In general, the new technologies and their application reduce the costs of governing, protecting the national security, and conducting business. However, technologies such as distributed computing and open system architectures are also making the information infrastructure and the information component of other infrastructures more vulnerable. Commercial markets alone now influence the deployment of advanced information technologies and DoD finds itself following that lead. Not only that, but, the market for information technology and services is clearly international in scope, creating an equivalence in information warfare capabilities among nations, terrorist groups, ethnic groups, and individuals.

- Finally, it is evident that **a very broad skill set is required to address these information warfare and information assurance policy and strategy issues**. Operational, intelligence, doctrinal, systems, networks, infrastructure, technology, political, diplomatic, business, and legal insights and experience are all drawn upon within the true scope of IW. Obviously, not every practitioner in every professional position requires all of them, but in these early stages of identifying and resolving the issues of this dawning information age, we must certainly have the capability to assemble and apply these diverse skills quickly to the topic of the moment.

Many of our nation's political and military leaders are deeply concerned about the dependency of key national security functions on vulnerable infrastructures. The issue is extremely complex and one which will not be resolved in 1 or 2 years. It will require extensive discussion involving representatives from many differing points of view—political, diplomatic, economic, military, commercial, and technical, to name a few. This report will help the Joint Staff better prepare to contribute to these discussions. The report is offered for the same purpose to the larger community to aid in addressing this national security issue of growing urgency and importance.

This page intentionally left blank.

Appendix A
Organizational Summaries

Appendix A Organizational Summaries

APPENDIX A
TABLE OF CONTENTS

Note: Organizational summaries have not been completed for these organizations. The organization is included in the index for possible future review.

TABLE OF CONTENTS (Continued)

Organization | Page

Interagency Groups

Advisory Committees

Note: Organizational summaries have not been completed for these organizations. The organization is included in the index for possible future review.

TABLE OF CONTENTS (Continued)

Note: Organizational summaries have not been completed for these organizations. The organization is included in the index for possible future review.

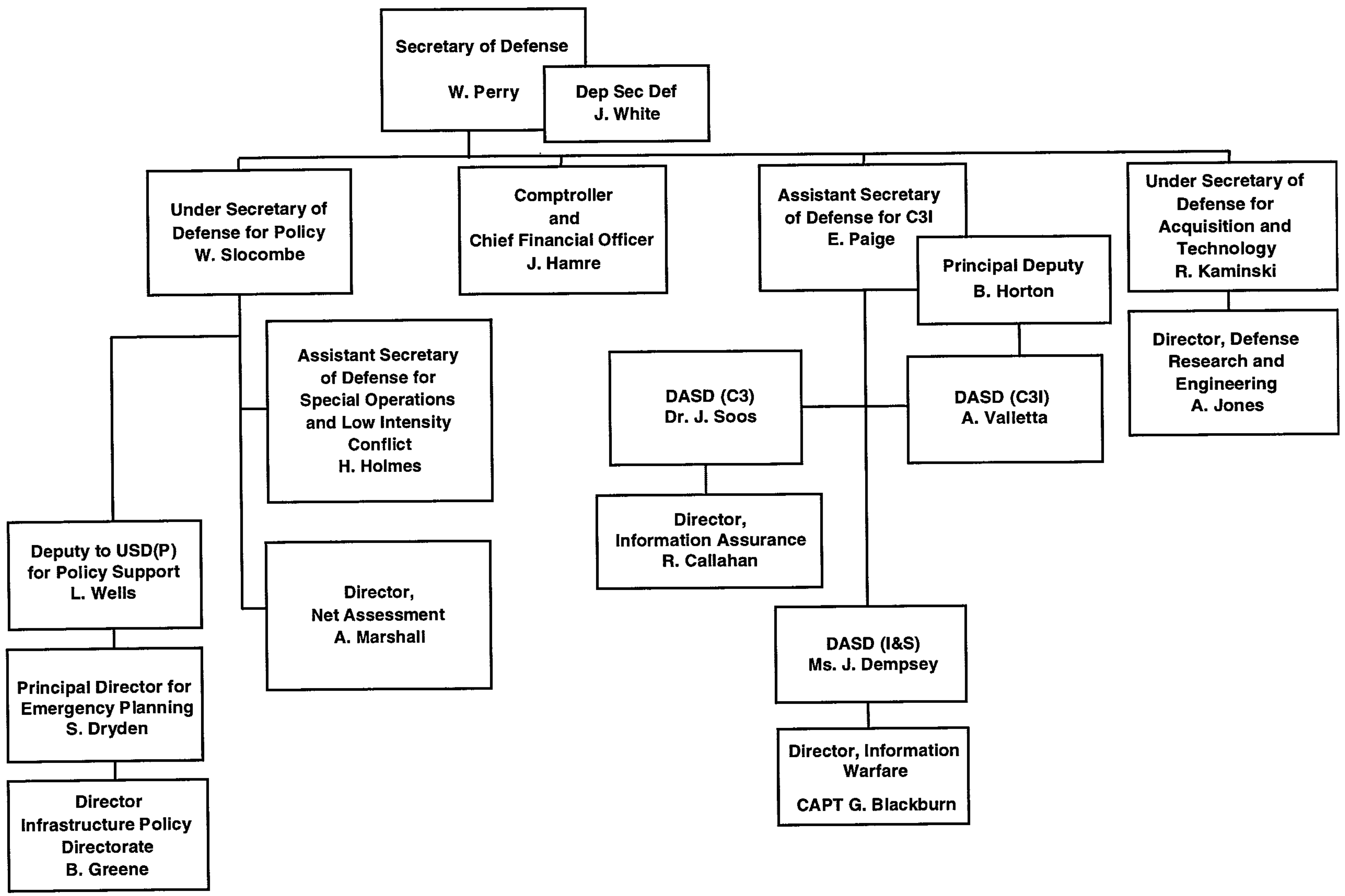
TABLE OF CONTENTS (Continued)

Note: Organizational summaries have not been completed for these organizations. The organization is included in the index for possible future review.

Department of Defense

Department of Defense

This page intentionally left blank.


Secretary of Defense W. Perry
Dep Sec Def J. White
Under Secretary of Defense for Policy W. Slocombe
Comptroller and Chief Financial Officer J. Hamre
Assistant Secretary of Defense for C3I E. Paige
Principal Deputy B. Horton
Under Secretary of Defense for Acquisition and Technology R. Kaminski
Director, Defense Research and Engineering A. Jones
Assistant Secretary of Defense for Special Operations and Low Intensity Conflict H. Holmes
Director, Net Assessment A. Marshall
Deputy to USD(P) for Policy Support L. Wells
Principal Director for Emergency Planning S. Dryden
Director Infrastructure Policy Directorate B. Greene
DASD (C3) Dr. J. Soos
Director, Information Assurance R. Callahan
DASD (C3I) A. Valletta
DASD (I&S) Ms. J. Dempsey
Director, Information Warfare CAPT G. Blackburn

Organization: Office of the Assistant Secretary of Defense (C3I)

Senior Information Assurance Official:

Emmett Paige, Assistant Secretary of Defense (C3I)

Information Assurance Points of Contact:

Roger Callahan, Director, Information Assurance
Captain Greg Blackburn, USN, Director, Information Warfare

On-Line Resources:

OASD(C3I) Homepage: http://www.dtic.dla.mil/defenselink/pubs/ofg/of_asdc3i.html

Information Assurance Related Missions and Functions:

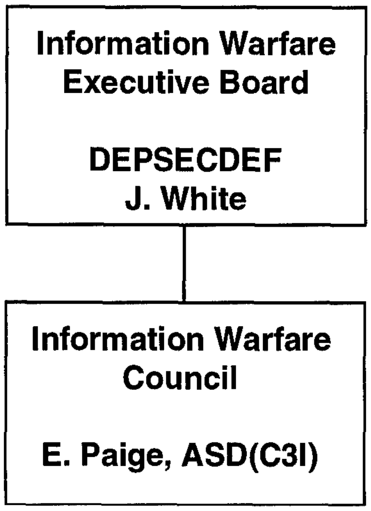
The ASD(C3I) has established a Directorate for Information Warfare to help the ASD(C3I) execute his task as the senior Information Warfare advisor to the Secretary of Defense and senior policy official in the Department for Information Warfare.

Information Assurance Activities, Issues, Best Practices, Lessons Learned:

- OMB has an Information Security Oversight Organization which was created under the provisions of Executive Order (EO) 12356, National Security Information.
- Current version of the Paperwork Reduction Act exempts DoD and intelligence activities from certain provisions for OMB oversight. Revision to Act may not provide these exemptions.
- Vulnerability of nation to information disasters is generally accepted. It is not clear what the responsibilities should be for dealing with the issues.
- The ASD(C3I) has requested an Intelligence Community Assessment and National Intelligence Estimate of the foreign Information Warfare threat with emphasis on the physical threat to the infrastructure supporting the Public Switched Network and the electronic threat to the information present on and accessible through the network. The assessment was published in July 1995. It is expected the National Intelligence Estimate will be completed in late 1996 or early 1997.
- The ASD(C3I) sponsored an executive forum in January, 1995, to discuss critical Information Warfare issues facing the DoD.

- The ASD(C3I) is revising the current DoD Directive 3600.1, Information Warfare, to reduce the classification and, thereby, increase knowledge and awareness of the Department's policy and responsibilities for IW.
- The ASD(C3I) is supporting an active Red Team effort with the USD (A&T).
- The ASD(C3I) has developed and is coordinating a formal "Defensive Information Warfare Strategy."
- The ASD(C3I) and the President, National Defense University are exploring ways for the NDU to assumė a central role in Information Warfare education and awareness.
- The USD(P) Office of Net Assessment and the ASD(C3I) have initiated a "Net Assessment of Information Warfare" as suggested by the Defense Science Board's 1994 Summer Study. Phase I of this Net Assessment will be completed by August 1996.
- The new Defense Planning Guidance (DPG) contains specific reference to enhancing Defensive Information Warfare/Information Assurance programs.
- The Deputy Secretary has established and will chair an Information Warfare Executive Board, supported by an IW Council. (See separate organizational summary for the IEWB.)
- The Deputy Secretary sponsored several "The Day After ..." games for members of his Executive Board and has invited members of the NSTAC Industry Executive Subcommittee, as well as other industry representatives to participate.
- The Deputy Secretary's IW Executive Board and ASD(C3I)'s Council will sponsor additional seminars, topical forums, and other events to bring the Department together with interested parties outside the Department to address critical Information Assurance issues.
- OASD(C3I) consider the past year a very successful year from the IW-D perspective:
  - Signing of PDD 39 and the creation of the Critical Infrastructures Working Group demonstrates high-level interest in infrastructure assurance.
  - A National HUMINT Directive has been published.
  - An Information Warfare Net Assessment is being conducted by OUSD(P)/NA.
  - USEUCOM deployed an operational IW-D team to Bosnia.
  - The Joint Command and Control Warfare Center has been exercising its Red Team capabilities.
  - Numerous CINC exercises and wargames provided many insights into tactics, doctrine, policy and organizational issues.
  - People are recognizing the need to share sensitive information -- offensive and defensive arms, intelligence and counter-intelligence, intelligence and operations.
  - Joint policy documents have been and are being published.
  - A Joint Mission Need Statement for Infrastructure Assurance Modeling has been coordinated by the Joint Staff (J6).
- OASD(C3I) initiated the Highlands Group to provide advice to the ASD(C3I) in information warfare concepts and their potential for revolutionary impact on DoD operations.

This page intentionally left blank.



Information Warfare
Executive Board

DEPSECDEF
J. White

Information Warfare
Council

E. Paige, ASD(C3I)

Organization: Information Warfare Executive Board (IWEB)

Senior Information Assurance Official:

John White, Deputy Secretary of Defense, Chairman

Information Assurance Points of Contact:

Emmett Paige, Assistant Secretary of Defense (C3I)
Captain Greg Blackburn, Executive Secretary, Director of Information Warfare, OASD(C3I)

On-Line Resources:

Information Assurance Related Missions and Functions:

The purpose of the Board is to provide a forum for the discussion and advancement of information warfare strategies, operations, and programs involving the Department of Defense.

The board is chartered to:

> Provide advice and recommendations to the DEPSECDEF and to the ASD(C3I) in his capacity as the DoD Information Warfare Manager.
>
> Provide for integrated development and consideration of IW policy, strategy, vulnerabilities and capabilities in all DoD activities, including formulation of IW recommendations for inclusion in the National Military Strategy, Defense Planning Guidance, and Contingency Planning Guidance.
>
> Eliminate gaps, identify overlaps, and ensure reciprocity in IW programs and operations.
>
> Serve as the forum for establishing coordinated DoD positions and recommendations on IW programs and operations, including interagency policy and strategy.
>
> Serve as the focal point for discussion of DoD IW policy, capabilities, and equities with national agencies, including recommending IW issues for consideration in the National Security Strategy.
>
> Improve participation of DoD corporate IW expertise and interests in the areas of policy, operations, intelligence, communications, and acquisition, both within the Department and at the national level.

Focus Department and national level information warfare strategy, capitalizing on information technology to accomplish national security goals and objectives.

Foster the development of training in IW concepts of operation, methodologies, potential vulnerabilities, and strategies for DoD and other national level entities.

Recommend new, or adjusted, DoD resource allocations consistent with IW policies and strategies.

Review plans and programs to ensure capabilities under consideration effectively and efficiently support IW policies and strategies.

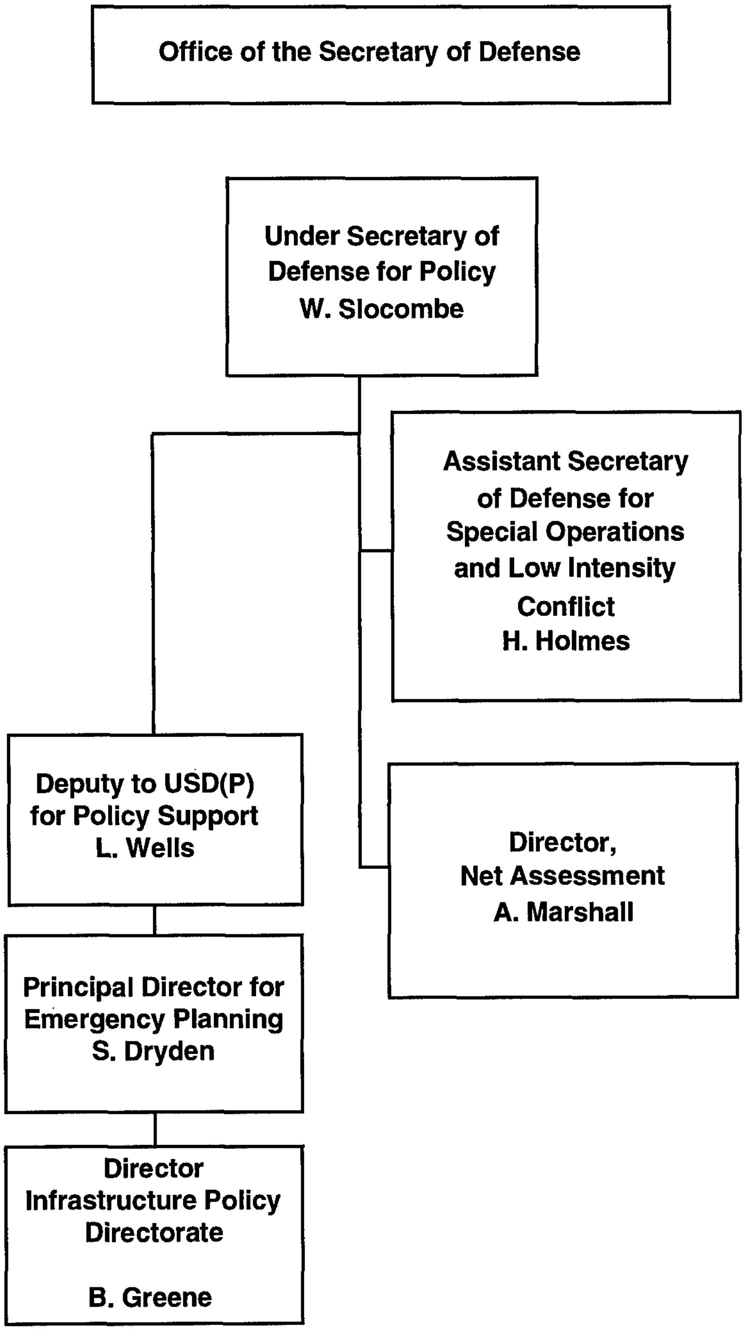
Membership of the IWEB includes:

Deputy Secretary of Defense (Chair)
Under Secretary of Defense (Acquisition and Technology)
Under Secretary of Defense (Policy)
Under Secretary of Defense (Comptroller)
Under Secretary of Defense (Personnel and Readiness)
Vice-Chairman, Joint Chiefs of Staff
Assistant Secretary of Defense for Command, Control, Communications and Intelligence
General Counsel of the Department of Defense
Vice Chiefs of the Military Services
Director, National Security Agency
Director, Defense Intelligence Agency
Director, Defense Information Systems Agency
Director, Program Analysis and Evaluation
Director, Information Warfare (Executive Secretary)
Deputy Director of Central Intelligence
Executive Director of the Central Intelligence Agency
National Security Council Executive

The IW Executive Board has a supporting Information Warfare Council (IWC) which will supervise supporting work for the Board. The IWC is composed of representatives designated by the IWEB representatives. The IWC also includes the Director of Special Programs, OUSD(A&T) and the Director of Net Assessment. Secretariat support for the IWEB and the IWC is provided by OASD(C3I). Other representatives from the Federal government may be invited to attend meetings as appropriate.

Information Assurance Activities, Issues, Best Practices, Lessons Learned:

- The Board will serve as the DoD focal point for IW discussion at the National level.
- The OASD(C3I) is exploring the establishment of an Information Assurance Group which will be subordinate to the IWC and will coordinate the ad hoc working groups being established to address IW issues such as threat, threat assessments, and indications and warning.



Office of the Secretary of Defense

Under Secretary of Defense for Policy
W. Slocombe

Assistant Secretary of Defense for Special Operations and Low Intensity Conflict
H. Holmes

Deputy to USD(P) for Policy Support
L. Wells

Director, Net Assessment
A. Marshall

Principal Director for Emergency Planning
S. Dryden

Director Infrastructure Policy Directorate

B. Greene

Organization: Infrastructure Policy Directorate, Office of the Under Secretary of Defense (Policy)

Senior Information Assurance Official:

Linton Wells, Deputy to the Under Secretary of Defense (Policy) for Policy Support

Information Assurance Points of Contact:

Sheila Dryden, Principal Director for Emergency Preparedness Policy
Brent Greene, Director for Infrastructure Policy

On-Line Resources:

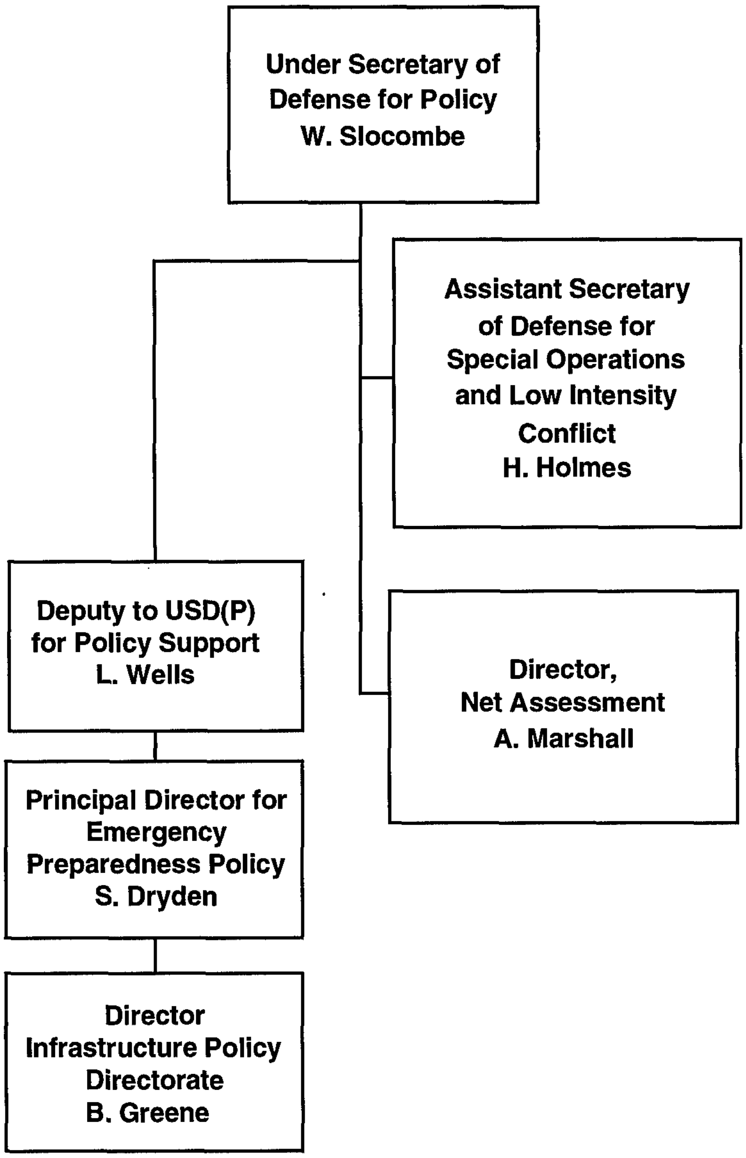
Information Assurance Related Missions and Functions:

The Infrastructure Policy Directorate is responsible for shaping policy issues pertaining to DoD infrastructure and future directions for information protection, including interagency and interdepartmental coordination.

Information Assurance Activities, Issues, Best Practices, Lessons Learned:

- Developed extensive "out-of-box" methodology for identifying dependencies within various infrastructures, critical nodes in the infrastructures, and dependencies among several infrastructures. Methodology includes modeling and simulation of industries and of the synergy between industries and infrastructures.
- Looking very closely at vulnerabilities of Supervisory Control and Data Acquisition (SCADA) networks.
- Need to add network and modeling and simulation expertise to our intelligence estimates.
- Concerned about how to insert infrastructure thinking into the Department of Defense processes - Defense Planning Guidance, Contingency Planning Guidance, National Military Strategy, National Security Strategy.
- Attempting to shape the role of DoD in the protection of infrastructures, including coordination between DoD and non-DoD government, and civilian/corporate owned/operated infrastructures.
- A National Defense Infrastructure Survivability Study was recently completed.
- The new-published Defense Planning Guidance directs the DoD components to investigate and assess their vulnerabilities and reliance on supporting infrastructures.

Office of the Secretary of Defense


Under Secretary of Defense for Policy W. Slocombe
Assistant Secretary of Defense for Special Operations and Low Intensity Conflict H. Holmes
Deputy to USD(P) for Policy Support L. Wells
Director, Net Assessment A. Marshall
Principal Director for Emergency Preparedness Policy S. Dryden
Director Infrastructure Policy Directorate B. Greene

Organization: Office of Net Assessments (OSD/NA)

Senior Information Warfare Official:

Director, OSD/NA, Andrew W. Marshall

Information Warfare Points of Contact:

COL Chuck Miller, USAF, Military Assistant
CAPT Jim FitzSimonds, USN, Military Assistant
CDR Jan van Tol, USN, Military Assistant
COL Scott Rowell, USA, Military Assistant

On-Line Resources:

Information Warfare Related Missions and Functions:

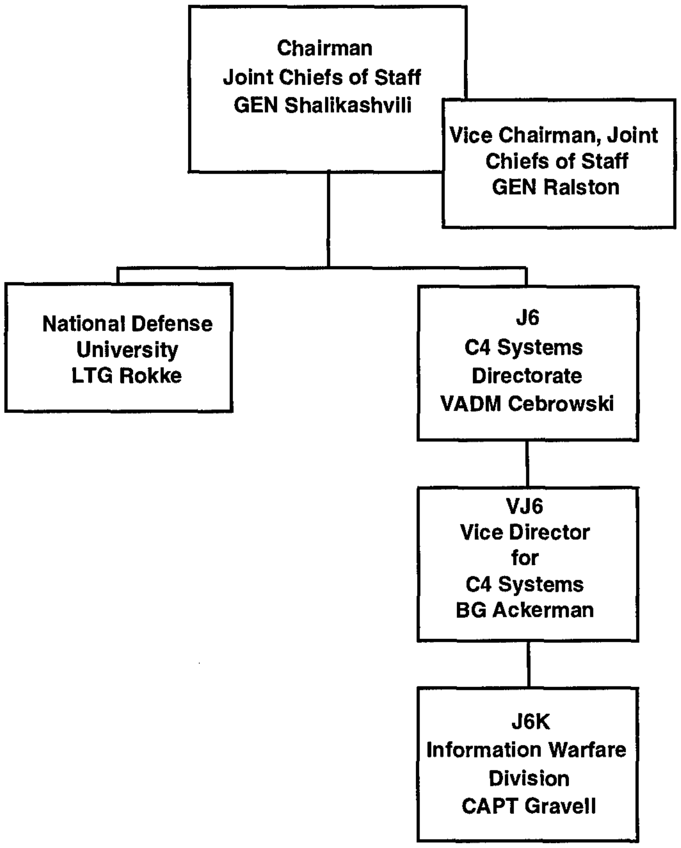
The Director of OSD/NA provides long-term analytic support to the Secretary of Defense and, when the SECDEF directs, to other senior officials in the Department (USD(P), USD (Acquisition), the Chairman, JCS, and the CINCs), on issues and trends in military affairs of potential import for the Department. Much of the analytic work of the office is engaged in preparing net assessments of the military balances in regions or in functional areas. The Director also makes recommendations regarding the DoD studies and analyses which are contracted outside the department. Information warfare was identified as a potentially important new warfare area several years ago in OSD/NA, and has been the subject of a widely ranging study effort ever since, within the office, and via contract, outside the office and with each of the Services and JCS.

Information Warfare Activities, Issues, Best Practices, Lessons Learned:

- The Defense Science Board Summer (1994) Study on Information Architecture for the Battlefield recommended a Net Assessment to be done in the Department on IW. Their assessment was begun earlier this year. OSD/NA has set up advisory panels of key people from within the military and JCS to advise as this work is executed. Colonel Miller is currently the POC in OSD/NA for the Assessment.

- In addition to the Net Assessment, there is a long-term study effort under way which involves a series of workshops, seminars (IW Infrastructure, MOEs, Gaming and Simulation, Training, Intelligence, etc.), and wargames (Dec., 93, Oct., 94), as well as efforts with ASD/C3I and the Intelligence Community to explore the dimensions of IW, policy and strategy issues for the Department, and the policy issues relating to agencies beyond DoD of importance for the Department.

THE JOINT STAFF



Organization: The Joint Staff

Senior Information Warfare Official:

VADM Arthur K. Cebrowski, J6

Information Warfare Points of Contact:

CAPT William Gravell, Division Chief, Information Warfare Division, J6K
Major Steve Spano, Information Warfare Division, J6K

On-Line Resources:

Joint Staff Homepage: http://www.dtic.mil:80/defenselink/jcs/

Information Warfare Related Missions and Functions:

J6K is responsible for all national information assurance and defensive information warfare programs and activities coordinated by the Joint Staff.

Information Warfare Activities, Issues, Best Practices, Lessons Learned:

- Ongoing training and education initiatives include implementing information warfare in exercises, coordinating Service training initiatives under the auspices of the Inter-Service Training Review Organization, and the conduct of an education strategy to infuse information warfare into the broad defense academic community by periodic visits to all engaged institutions.
- CJCSI 6510.01A, *Defensive Information Warfare Implementation*, has been produced and signed out. This builds upon broad policy in CJCSI 3210.01, *Information Warfare Policy*. Both were produced within the last year.
- The Joint Warfighter Capability Assessment (JWCA) process includes studies of information warfare offensive and defensive capabilities, emerging technologies, and intelligence support to IW. Additionally, the JWCA includes an effort to examine Service and Agency Program Objective Memorandum submissions relative to the Defense Planning Guidance and CINC requirements.
- J6K is studying nascent technologies outside of the requirements process to determine if some may have information warfare applications. The results of this study are provided in two documents:
  - Institute for Defense Analyses, *Information Warfare Technologies: Survey of Selected Civil Sector Activities*, IDA Document D-1792, February, 1996.
  - Institute for Defense Analyses, *Information Warfare: Selected Long-Range Technology Applications*, IDA Paper P-3157, February, 1996.
- J6K is leading an effort to develop rigorous modeling and simulation capabilities that would support CINC requirements for awareness of vulnerabilities of supporting national infrastructures. A Mission Needs Statement (MNS) for this capability is in final coordination.

- J6K is reexamining multi-level security (MLS) concepts and requirements and incorporating these concepts into information protection architecture efforts. J6K is working with the CINCs to define new MLS requirements and refine existing MLS requirements, and is establishing development and fielding priorities. These efforts are being validated by and within the JWCA process.
- The Joint Staff J6 recently completed an informative brochure entitled *Information Warfare, Implementing the Vision.* The brochure includes an IW-D implementation model which serves as an organizing construct for IW-D issues and activities.
- Preparation of Joint Doctrine for IW, Joint Pub 3-13, has been initiated. Joint Staff (J3) has the overall lead, with J6 responsible for defensive aspects and acting as technical review authority on the total effort.
- J6 is sponsoring a comprehensive examination of national IW-D issues by the Defense Science Board Task Force on Information Warfare Defense. The Task Force will report out in August 1996.

Organization: School of Information Warfare and Strategy (SIWS), Advanced Concepts, Technologies, and Information Strategies Directorate, Institute for National Strategic Studies, National Defense University (NDU)

Senior Information Warfare Official:

LTG Rokke, President, National Defense University
Dr. Hans Binnendjjk, Director, Institute for National Strategic Studies
Dr. David S. Alberts, Director, Advanced Concepts, Technologies, and Information Strategies
Dr. John Alger, Director, School of Information Warfare and Strategy (SIWS)

Information Warfare Points of Contact:

Col. (USMC, Retired) Bradley E. Barriteau, Professor, SIWS
Tom Czerwinski, Professor, SIWS
CDR Lee J. Ducharme, USN, Professor, SIWS
Lt. Col. Richard L. Casey, USAF, Executive Officer, SIWS
Dr. Fred Giessler, Professor, SIWS
Dr. Dan Kuehl, Professor, SIWS

On-Line Resources:

NDU Homepage: http:\\www.ndu.edu

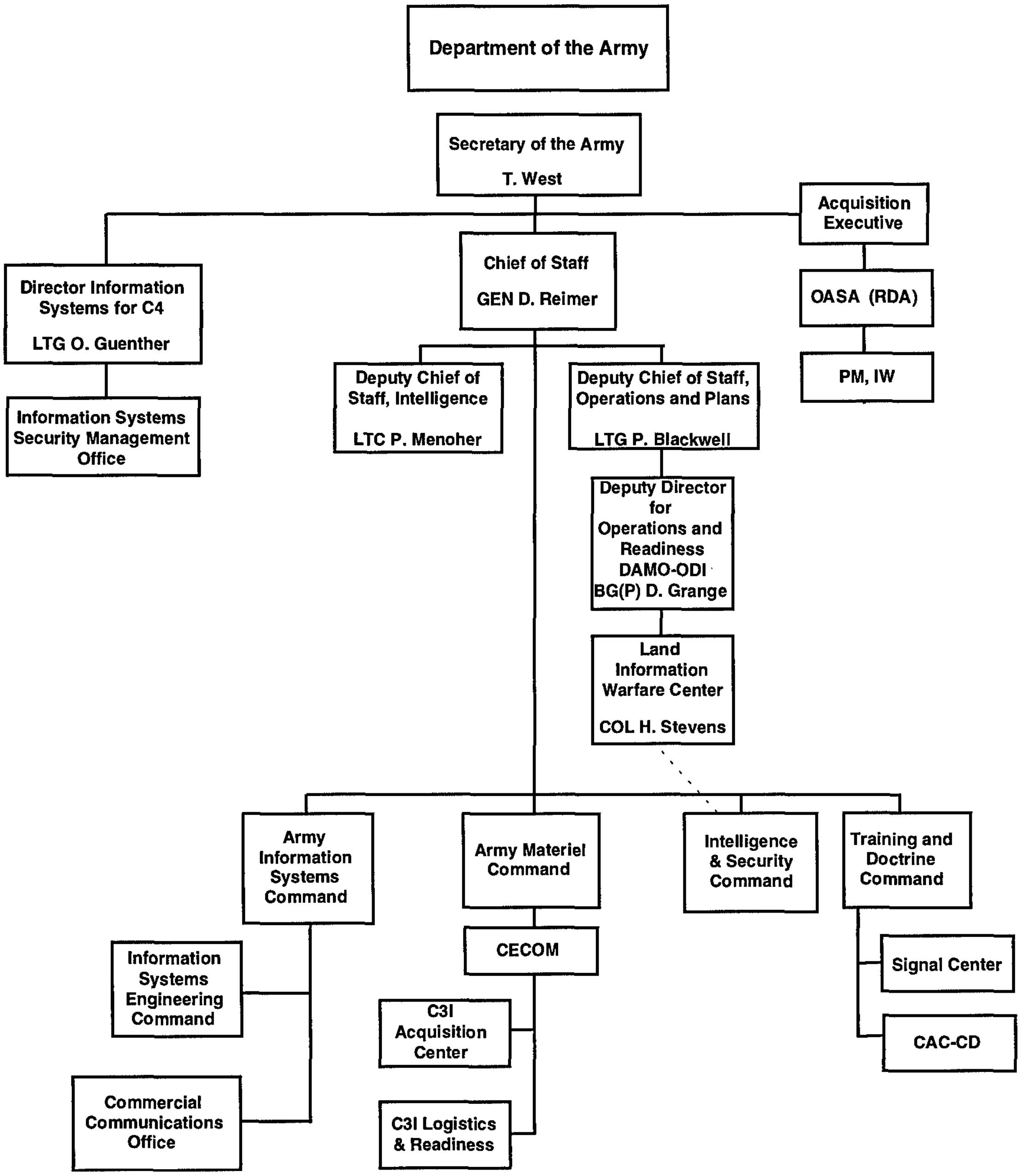
Information Warfare Related Missions and Functions:

The School of Information Warfare and Strategy graduated 32 students from its 10-month senior level (war college) program on 12 June 1996. The event marked the termination of the JCS-directed 2-year pilot as a stand alone senior-level program dedicated to the study of the information component of national power, but in recognition of the importance of information strategies, the President of the University has established a 3-tier program of information studies at the University. In the first tier, all colleges of the University will incorporate information studies into their curricula as appropriate to their respective missions. In the second tier, a slate of information strategies focused advanced studies will be offered to all senior-level students at the National Defense University, and in the third tier, an information strategies concentration program will be offered under the aegis of the School of Information Warfare and Strategy. The School of Information Warfare and Strategy will continue to offer its very popular 5-day Introduction to Information-Based Warfare Course for O-4, equivalents, and above and a 2-day executive course for O-6, equivalents, and above, which was first offered in April 1996. The School also offers a 2-day course in Chaos Theory for the Warrior.

Information Warfare Activities, Issues, Best Practices, Lessons Learned:

- The combined force of the School of Information Warfare and Strategy and the Center for Advanced Concepts and Technology provides a center of excellence for the Department of Defense in the teaching and research of information warfare concepts. The combining of formerly separate research and teaching organizations results in the directorate of Advanced Concepts, Technologies, and Information Strategies. In addition to its teaching and research roles, this directorate is heavily engaged in outreach activities. It sponsors several conferences and workshops each year on topics germane to information warfare, and its members often speak on a variety of topics relevant to information warfare.

This page intentionally left blank.


Department of the Army
Secretary of the Army
T. West
Acquisition Executive
Director Information Systems for C4
LTG O. Guenther
Chief of Staff
GEN D. Reimer
OASA (RDA)
Information Systems Security Management Office
Deputy Chief of Staff, Intelligence
LTC P. Menoher
Deputy Chief of Staff, Operations and Plans
LTG P. Blackwell
PM, IW
Deputy Director for Operations and Readiness DAMO-ODI
BG(P) D. Grange
Land Information Warfare Center
COL H. Stevens
Army Information Systems Command
Army Materiel Command
Intelligence & Security Command
Training and Doctrine Command
Information Systems Engineering Command
CECOM
Signal Center
C3I Acquisition Center
CAC-CD
Commercial Communications Office
C3I Logistics & Readiness

Organization: Department of the Army

Senior Information Warfare Officials:

LTG Paul E. Blackwell, Deputy Chief of Staff, Operations and Plans
LTG Paul E. Menoher, Deputy Chief of Staff, Intelligence
LTG Otto J. Guenther, Director of Information Systems for C4 and Chief of Information

Information Warfare Points of Contact:

LTC Craig Jones, DAMO-ODI, ODCSOPS
Donal Harrison, DAMI-ST, ODCSINT
Phillip J. Loranger, Chief Command and Control Protect Division, Army Information Systems Security Management Office (ISMO), ODISC4

On-Line Resources:

Army Homepage: http://www.army.mil/default.htm
Army ODISC4: http://www.army.mil/disc4-pg/disc4.htm

Information Warfare Related Organizations, Missions and Functions:

Headquarters, Department of the Army formed a Command and Control Protect (C2 Protect) triad consisting of the Deputy Chief of Staff for Operations and Plans (DCSOPS), Deputy Chief of Staff for Intelligence (DCSINT), and the Director of Information Systems for Command, Control, Communications and Computers (DISC4) to "integrate C2 Protect into all facets of military operations." [HQDA 1]

DCSOPS: DCSOPS has proponency for Information Warfare and addresses force modernization issues related to IW. Operational issues concerning IW are handled within the Directorate for Operations, Readiness, and Mobilization (DAMO-OD). The Directorate for Strategy, Plans, and Policy (DAMO-SSP) is responsible for coordinating IW policy in the Army while the Directorate for Force Development is responsible for coordinating and prioritizing IW requirements for the Army. DAMO-ODI is charged with operational management of the Army's Command and Control Operations and has oversight of the Land Information Warfare Activity's operations.

> Land Information Warfare Activity (LIWA): Established in March, 1995 at Fort Belvoir, Virginia, the LIWA, assigned to the U.S. Army Intelligence and Security Command, is under the operational control of DAMO-ODI, DCSOPS. An organizational summary for the LIWA follows.

DCSINT: In coordination with DCSOPS and DISC4, DCSINT is responsible for threat definition, establishment of policy and integrating counter-intelligence support to protect command, control, communications and computers.

DISC4: In coordination with DCSOPS and DCSINT, DISC4 is responsible for implementing procedural and material protective measures, to protect command, control, communications and computers and for the development, sustainment and management of the C2 Protect Library.

> Information Systems Security Management Office (ISMO) is subordinate to ODISC4. The mission of ISMO is to implement protective measures, both procedural and material, to protect Army command and control and implement lead responsibilities for the development, sustainment and management of the C2 Protect Plans.

Training and Doctrine Command (TRADOC) has established a Space and C2W Directorate to oversee IW related actions.

Information Warfare is integrated across the Army and implemented in the Force XXI initiative, therefore all Major Commands (MACOM) and other Army organizations are involved in planning, developing and implementing C2 Protect measures in the Army.

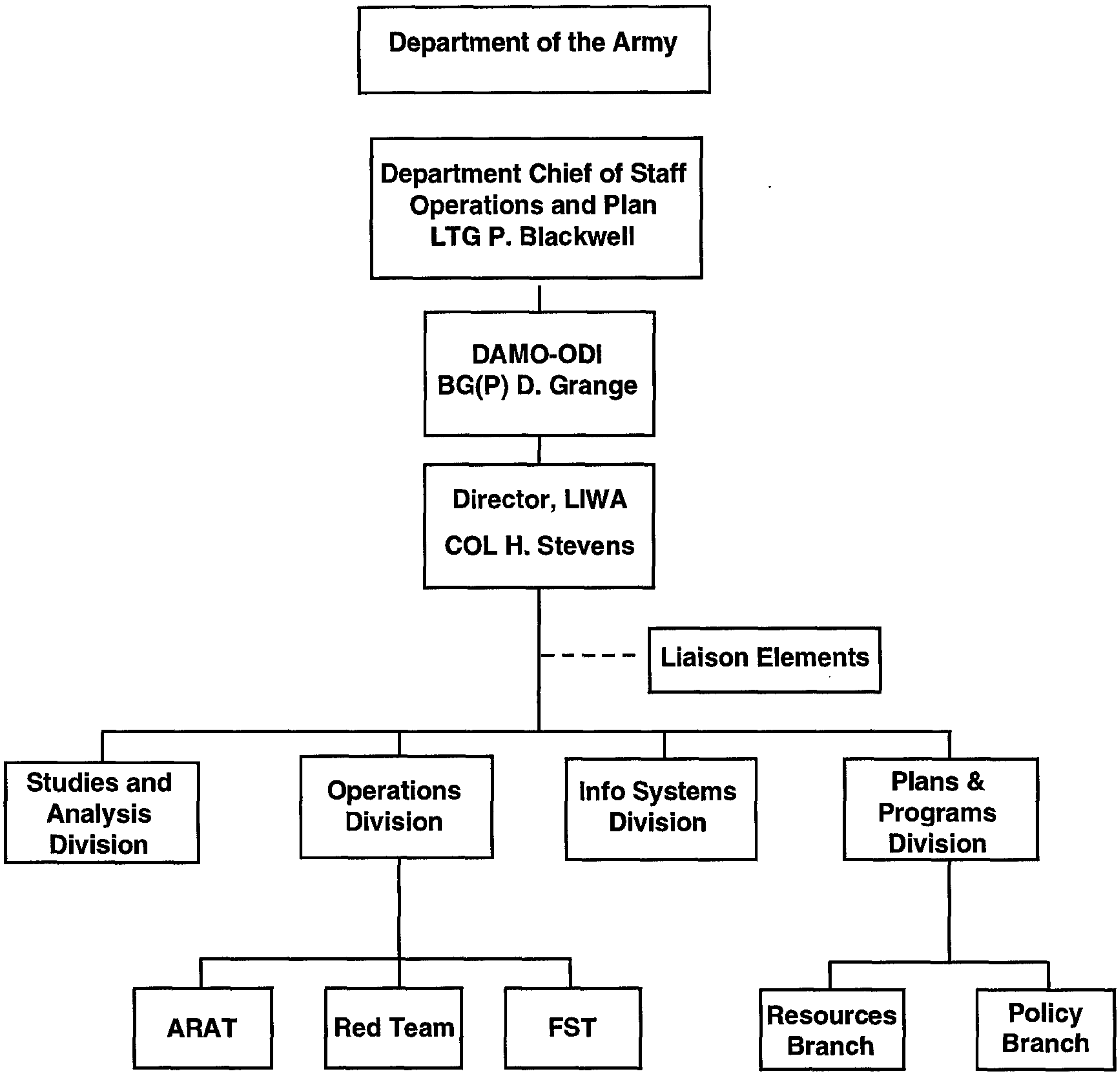
Information Warfare Activities, Issues, Best Practices, Lessons Learned:

- The Army has adopted Information Operations (IO) doctrine and is integrating IO into Army doctrine, individual and unit training, leader development, force design, and material acquisition initiatives. TRADOC has published Field Manual 100-6, *Information Operations*, 15 April, 1996 [HQDA 2] The Army has adopted Information Operations for two reasons: to recognize that information issues permeate the full range of military operations (beyond the traditional context of war), from peace through global war; and to emphasize the tactical and operational aspects of information based warfare. Information Operations integrate all aspects of information to support and enhance the elements of combat power, with the goal of dominating the battle space at the right time, at the right place, and with the right weapons or resources. The Army supports or implements Information Warfare through Command and Control Warfare (C2W) actions." [HQDA 2] The components of IO are military information systems, intelligence, and command and control warfare. The IW-D component of IO is C2-Protect. The Army has adopted a risk management approach and stresses risk management over risk avoidance.
- The Army is using several steering groups and working groups as to help execute, and integrate information warfare across the Service and to provide executive oversight of the program. The IW General Officer Steering Group is chaired by the DAMO-OD, DCSOPS and includes representatives charged with implementing IW. The C2 Protect General Officer Steering Group is co-chaired by the DCSINT and the DISC4 and includes general officers from DCSOPS and the signal and acquisition communities. Established in late 1993, a C2 Protect Council of Colonels was formed to deal with the increasing burden of protecting the wide range of C2 assets essential to the success of IW. The Council, chaired by ISMO, meets quarterly and addresses current Army C2 Protect issues.
- In January 1995, the DISC4 established an Army C2 Protect Working Group and tasked it to develop the C2 Protect Library. Membership includes a broad range of Army organizations. The C2 Protect Library consists of six volumes:

VOL 1 C2 Protect Program Management Plan, August 1995
VOL 2 C2 Protect Master Training Management Plan, 18 January 1996
VOL 3 C2 Protect Implementation Plan, 29 February 1996
VOL 4 Intelligence Support C2 Protect Action Plan, Draft
VOL 5 C2 Protect Resourcing Proposal, May 1996, Draft
VOL 6 A C2 Protect Automation Threats Overview, SECRET, 14 February 1996.

Volumes 1, 2, 3, 6 have been published. Volumes 4 and 5 are in draft. In addition to the C2 Protect Library, key Army regulations for information security (AR 380-19), intelligence requirements (AR 381-11), and acquisition (AR 25 and 70) have been revised to incorporate C2 Protect. Additionally, the Army is issuing policy messages directing C2 Protect tactics, techniques, and procedures.

- Protect: The Army is leveraging the efforts of DISA and the other Services to provide system administrators with the capability to scan and monitor systems, to audit systems and reduce audit data, to identify and patch system vulnerabilities, to eradicate viruses, and to implement password protection programs. It has identified and issued two automated sets of tool boxes for use by Automated Information System Mangers to help them protect their information environments. Also, the Army co-chairs, with DISA, the OSD Common Tools Working Group and advises the Army organizations of tools available from DISA and of the services provided by the DISA ASSIST Help Desk.
- Training, Education and Awareness: In addition to the training necessary for the unique technical skills required for LIWA operations, the Army has established training for system administrators and information system security managers. Awareness training is provided for users and includes executive level training.
- Acquisition: Increased emphasis is being placed on embedding security into development programs. Efforts include revised acquisition regulations with stiffer security requirements, monitoring of Major Automated Information System Review Council (MAISRC) programs, and closer attention paid to requests for security waivers. The Department of the Army Technical Architecture (ATA), published on 30 January 1996, applies to all systems that produce, use, or exchange information electronically and includes information security standards. The ATA was used as a model for the recently published draft Joint Technical Architecture. The Army Enterprise Strategy, the Army Modernization Plan, and the ATA provide broad, high level information warfare and C2 Protect guidance for program developers.
- Resourcing: The C2 Protect Resourcing Proposal (VOL 5 of the C2 Protect Library) is in Final Draft. This volume, in concert with the other volumes of the Plan, defines the c2 Protect program resourcing instructions and justification for resourcing all twelve C2 Protect initiatives. In the short term, implementation of the C2 Protect program has outpaced resources.


Department of the Army
Department Chief of Staff Operations and Plan LTG P. Blackwell
DAMO-ODI BG(P) D. Grange
Director, LIWA COL H. Stevens
Liaison Elements
Studies and Analysis Division
Operations Division
Info Systems Division
Plans & Programs Division
ARAT
Red Team
FST
Resources Branch
Policy Branch

Organization: Land Information Warfare Activity (LIWA)

Senior Information Warfare Official:

COL Halbert Stevens, Commander, LIWA

Information Warfare Points of Contact:

LTC Tom Hudson, Deputy Commander, LIWA

On-Line Resources:

Information Warfare Related Organizations, Missions and Functions:

Established in March, 1995 at Fort Belvoir, Virginia, the LIWA, assigned to U.S. Army Intelligence and Security Command, is under the operational control of DCSOPS. The mission of the LIWA is to provide Department of the Army level Information Warfare/Command and Control Warfare support to Land Components and separate Army commands to facilitate planning and execution of information operations. The LIWA coordinates with National, Joint, and Service IW/C2W centers to exchange and synchronize intelligence and information support across the operational continuum. The LIWA provides supports teams to facilitate operational planning and is responsible for conducting Army vulnerability assessments, providing computer emergency response, and Red Teaming.

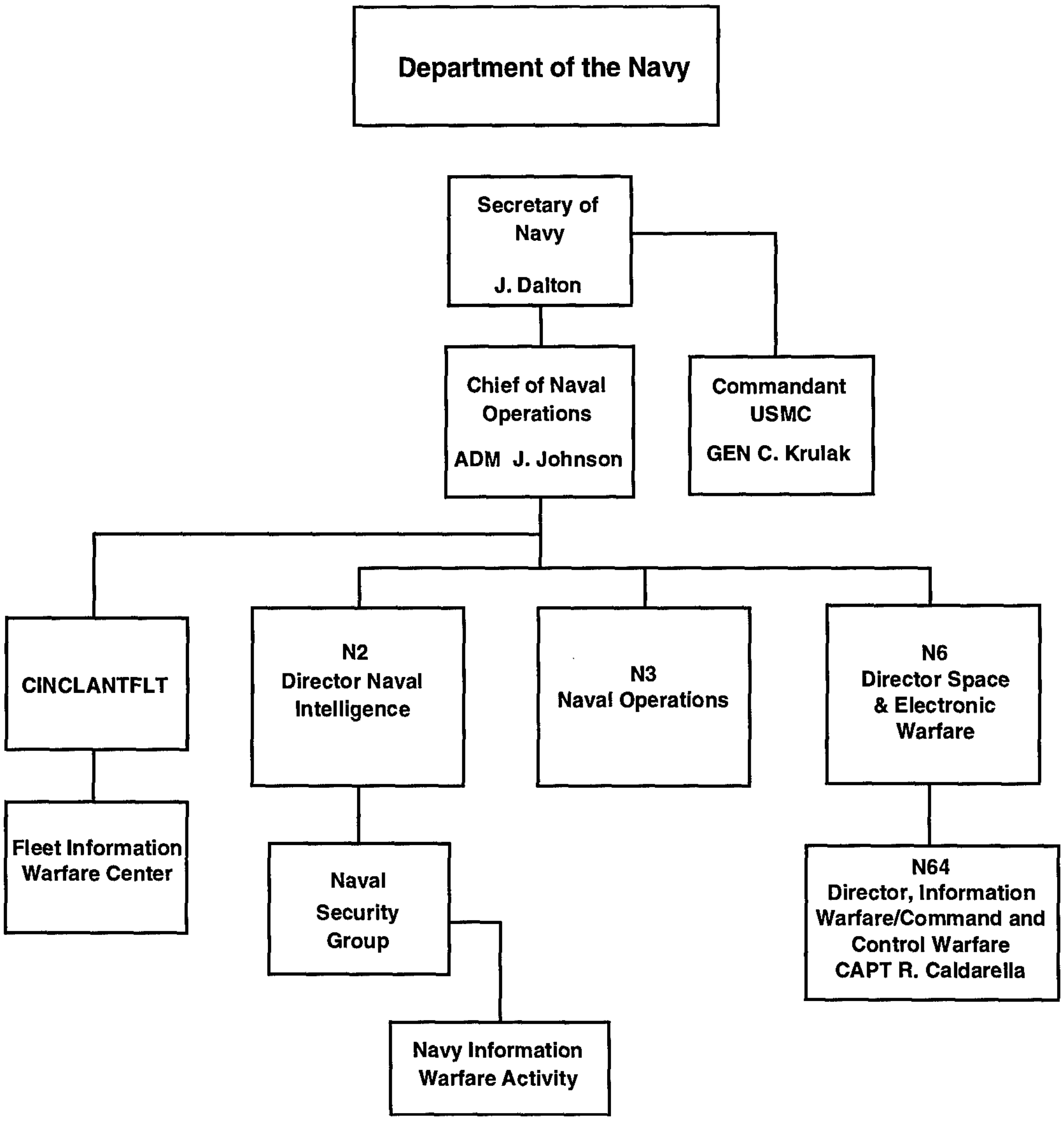
Information Warfare Activities, Issues, Best Practices, Lessons Learned:

- The Army is in the process of incorporating LIWA capabilities into day-to-day operations. LIWA capabilities are addressed in the FM 100-6 [HQDA 2] and an official Table of Distribution and Allowance; to refine LIWA staffing, is being developed.
- A key mission of the LIWA is to provide computer emergency response support to Army forces. To meet the increasing demand for computer emergency response, the Joint Requirements Oversight Council (JROC) recommended that the Army develop an organic computer emergency response capability similar to the capabilities of the other Services. The LIWA is building the Army central emergency response capability and will soon become a member of the Forum of Incident Response and Security Teams (FIRST). LIWA is also building the Continuity of Operations (COOP) site for the DISA ASSIST. The Army is implementing a centralized react and reporting capability. This includes finalizing an MOU with DISA with respect to incident reporting and collocating and integrating computer security skills with the four Army Regional Network Management Centers. Augmenting these with counterintelligence, law enforcement, and legal assets is under consideration. The first Regional CERT was established in USAREUR on 1 February, 1996. It currently supports the European Theater to include Operation Joint

Endeavor and uses an Automated Intrusion Monitoring System (AIMS) tool to monitor theater hosts.

- VAAP: The Army has adopted the DISA Vulnerability Assessment and Analysis Program (VAAP). Findings and fixes are promulgated by the Army staff and incorporated into tactics, techniques and procedures. DISA provides VAAP support for the sustaining base and LIWA for the tactical environment.
- Red Teaming: LIWA is building a capability to provide Red Teaming support for the Army in the field. The Army Digitization Office (ADO) has the lead for TF XXI. ADO uses LIWA assets for TF XXI Red Teams.

This page intentionally left blank.


Department of the Navy
Secretary of Navy
J. Dalton
Chief of Naval Operations
ADM J. Johnson
Commandant USMC
GEN C. Krulak
CINCLANTFLT
N2
Director Naval Intelligence
N3
Naval Operations
N6
Director Space & Electronic Warfare
Fleet Information Warfare Center
Naval Security Group
N64
Director, Information Warfare/Command and Control Warfare
CAPT R. Caldarella
Navy Information Warfare Activity

Organization: Department of the Navy

Senior Information Warfare Officials:

VADM J. P. Reason, Deputy Chief of Naval Operations for Plans, Policy and Operations (N3/N5)
VADM W. J. Davis, Jr., Director, Space, Command and Control, and Information Warfare (N6)
RADM T. F. Stevens, Commander, Naval Security Group Command/EA for IW

Information Warfare Points of Contact:

CAPT R. J. Caldarella, Director, Information Warfare/Command and Control Warfare Division (N64), Office of the Chief of Naval Operations
CAPT M. V. Sherrard, Deputy Director, Information Warfare/Command and Control Warfare Division (N64B), Office of the Chief of Naval Operations
E. Owen, Defensive Information Warfare Branch (N643), Information Warfare/Command and Control Warfare Division, Office of the Chief of Naval Operations
CDR J. Stratton, Staff Ops & Plans, Special Warfare Objective (OPNAV N513)
CDR E. Kanerva, Assistant Chief of Staff for IW/C2W, CNSG (CNSG N6)

On-Line Resources:

Navy Homepage:	http://www.navy.mil
FIWC NAVCIRT Homepage:	http://www.fiwc.navy.mil
NRL Homepage:	http://www.cmf.nrl.navy.mil

Information Warfare Related Organizations, Missions and Functions:

The Deputy Chief of Naval Operations for Plans, Policy and Operations (N3/N5) is responsible for developing Navy IW/C2W policy, strategy and operational concepts including operations security (OPSEC).

The Director, Space, Command and Control, and Information Warfare (N6) is responsible for overall IW/C2W development and implementation guidance to include establishment of IW/C2W objectives and procedures. The Information Warfare/Command and Control Warfare Division (N64) is responsible for the development of requirements, plans, and IW programs in the Navy. The office is the day-to-day point of contact for all IW matters in the Navy. Inside N64, the Defensive Information Warfare Branch (N643) serves as sponsor of the Navy INFOSEC Program including program development, implementation, planning, and budgeting.

The Commander, Naval Security Group, serves as CNO's (N6) Executive Agent (EA) for Navy IW, overseeing all manpower, training, and equipment requirements that are associated with IW. The IW EA, in coordination with CNO N6/N8, the Navy Systems Commands, and other appropriate agencies, reviews and documents requirements for development, procurement, training, deployment, and life cycle support of Navy IW systems. Additionally, the IW EA, in conjunction with the Chief of Naval Education and Training, Naval Doctrine Command, and the Fleet Information Warfare Center (FIWC), is responsible for ensuring IW doctrine and concepts, including IW protect, is included in appropriate Navy training programs for Navy personnel throughout their careers.

The Space and Naval Warfare Systems Command has established a program directorate (PD-16) for Information Warfare. PD-16's mission is to develop, procure, field, and support interoperable Navy IW systems. PD-16 additionally serves as the Navy INFOSEC execution agent for DoN and DoD/National agencies. A primary function of PD-16 is to serve as the Navy's single point of entry into the IW acquisition community. PD-16 is supported by three program managers who manage the development, acquisition, integration, and life cycle support of programs for navy IW systems. IW protect systems are managed by PMW 161, the Information Systems Security (INFOSEC) Program Office. PMW 161 is the designated point of contact for DoN interface with NSA for all key management, embedded crypto, and other INFOSEC matters.

The Office of Naval Intelligence (ONI) is the focal point for intelligence and threat support to Navy-related IW/C2W programs and coordinates with the intelligence community for satisfaction of Navy IW/C2W requirements. ONI will also develop all source intelligence indicators that will contribute to establishing Measures of Effectiveness for Navy IW/C2W tactics and weapons.

The Fleet Information Warfare Center (FIWC), established 1 Oct 1995, is the Navy's IW Center of Excellence, and is the principle agent for development of IW/C2W tactics, procedures, and training. FIWC deploys personnel trained in IW protect disciplines and equipped with appropriate hardware, including C-2 protect hardware and software systems, to support battle group and joint task force operations. Additionally, FIWC provides Navy Computer Incident Response Teams (NAVCIRT), and acts as the Navy's single point of contact for information systems monitoring, leveraging capabilities found in the reserves and NSGA Pensacola.

The Naval Information Warfare Activity (NIWA), acts as CNO's technical agent for the pursuit of information warfare related technologies. As such, NIWA conducts technical threat analysis and vulnerabilities assessment studies, develops technical requirements for, and evaluates/assesses new information technologies, competitive architectures, and advanced concepts for Navy defensive IW systems.

The Director, Communications Security Material System, a third echelon command under COMNAVCOMTELCOM, acts as the Central Office of Record for DoN assurance hardware and software.

Reflecting the cross-cutting nature of IW/C2W, implementing instructions assign responsibilities across the full spectrum of Navy command and staff activities. The organizations and functions described above reflect key Navy organizations responsible for implementing and institutionalizing IW/C2W in the Navy. In addition to these, the Fleet CINCs, Numbered Fleet Commanders, and Battle Group Commanders have IW/C2W Commanders and a supporting staff assigned. A portion of this staff is dedicated to IW defensive issues, including the protection and assurance of information systems and the data contained therein.

Information Warfare Activities, Issues, Best Practices, Lessons Learned:

- The Navy subscribes to the direction provided in DoD Instruction TS3600.1 and CJCS MOP 30. The Chief of Naval Operations (CNO) IW-D strategy includes investment in protective technologies; reform of the acquisition process, operational integration of the security disciplines, and use of a risk management process rather than a risk avoidance. An update of the Navy (DoN) policy OPNAVINST 5239.xx will require that all information services (voice, video, imagery, data) be protected; that all unclassified systems be considered sensitive; and requires all sensitive systems to implement network security management tools to monitor, detect, isolate, and react. DoN policy also requires all classified systems, in addition to encryption, to implement identification/ authentication and network security management tools. Two key documents issued by the CNO are OPNAVINST 3430.25, Information Warfare and Command and Control Warfare, April 1994, which established Navy IW policy and assigned responsibilities, and OPNAVINST 3430.26, Implementing Instruction for Information Warfare/Command and Control Warfare (IW/C2W), 17 January 1995 which issues implementing guidance and organizational relationships. Overall doctrine for IW/C2W is found in Navy Doctrine Publication (NDP) 3, *Naval Operations.* The Fleet Information Warfare Center (FIWC), in conjunction with the Naval Doctrine Command, is developing specific IW/C2W doctrine to be promulgated in the following publications:

    - Naval Warfare Pub 3-13 (Naval IW)
    - Naval Warfare Pub 3-13.1 (Naval C2)
    - Naval Warfare Pub 3-14.1.1 (Navy C2W/C2W Commander's Manual).

- Panels and Working Groups: The Navy has established a Navy Information Warfare Council to foster closer working relationships between Navy organizations responsible for Navy IW program planning and execution, and to institutionalize IW throughout the Navy. The council is comprised of the senior 0-6 from each of the key Navy commands supporting IW. Additionally, specific Navy organizations have established internal working groups to help implement IW/C2W. The N3/N5 has established a Strategic Planning Cell to develop and coordinate OPNAV IW/C2W strategy and policy. The INFOSEC Engineering Working Group (IEWG), chaired by SPARWAR PMW-161, consists of senior engineers from system command, laboratories, and contractors and establishes technical strategies for the Information Assurance/INFOSEC Program. Additionally, OPNAV N643 chairs a Vulnerability Assessment, Countermeasures Tools Working Group that will consolidate and focus Navy resources to upgrade and expand assessment and monitoring capabilities.

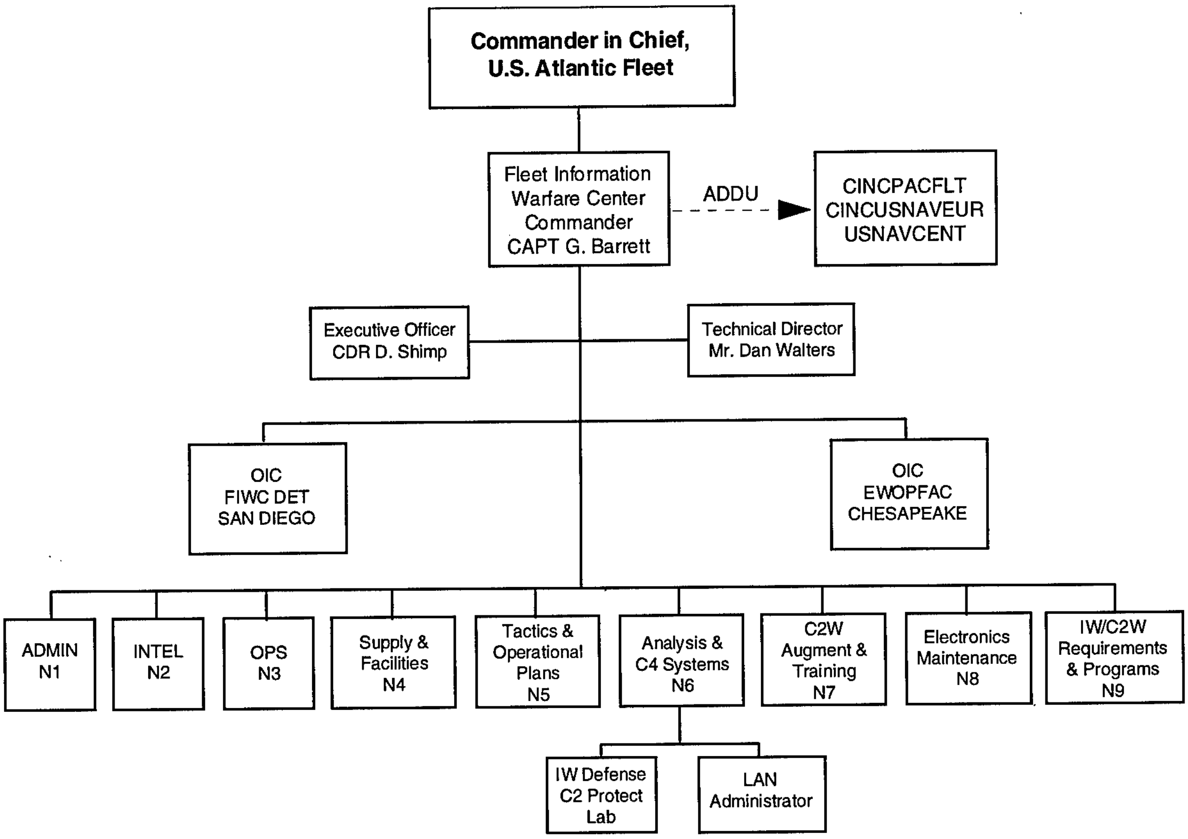
- Protect and Detect: The Naval Research Laboratory (NRL) took the publicly available S/Key™ onetime password system developed by Bellcore, added a stronger algorithm, then released the code back to the Internet. A variety of Navy and other DoD sites are using the NRL enhanced system to provide much stronger hacker protection for hosts and firewalls. The Navy is pursuing crypto options for Shipboard Secure Phone and participating in the Digital Voice Processor Consortium. A priority long term effort is to enhance the security protocols that will be used on the Fleet Internet. NRL will develop and implement standardized security mechanisms for the next generation of the Internet that will make COTS products available to the Navy and DoD with the appropriate security attributes. NRL security protocols are included in the Internet Protocol, version 6 (IPv6) proposal. The security mechanisms are algorithm-independent and support both commercial and military needs. The Navy/USMC has identified funds within their POM which sufficiently cover firewalls and guards as required to protect their connections to DISN. They have also funded for their internal needs. The Navy is modifying the Ice Pick™ tool with NRL technology to allow a central administrator to probe a PC network for vulnerabilities.

- Training, Education and Awareness: The Chief, Naval Education and Training (CNET) (N7) is designated as lead for IW training, formally referred to as DoD Interservice Training Review Organization (ITRO) Initiative for Joint IW Training (DITJIT) as of May 1995. The following training programs have been developed and/or have been initiated:

  – Awareness Training - Basic to Master level program consisting of:
    - * Basic Officer and Enlisted "A" School "Introduction to IW/C2W"
    - * Department Head/Journeyman Level Schools "Fundamentals of IW/C2W"
    - * CO/XO and Enlisted Master Level School "IW/C2W Advanced Application"
    - * Specialized Modules Training - A four element program consisting of
      - ◊ IW/C2W for Intel Pros
      - ◊ IW/C2W for USN/USAF EWOs
      - ◊ IW/C2W Common Core CBT
      - ◊ Formal Schools - "Retooled"
        - -- "Network Security & Vulnerability Technician"
        - -- "Nodal Analysis Technician"
        - -- DoD-Common COI for System/Network
    - * Administrators

- Acquisition: The Navy will direct the incorporation of security standards in Navy programs via a proposed SECNAV Instruction 5200.1-M, Naval Program Protection Plans. Non-centrally purchased AIS will be required to incorporate standard INFOSEC products and procedures. In addition, the Navy will establish a realistic vulnerability assessment/certification and accreditation process.

This page intentionally left blank.


Commander in Chief,
U.S. Atlantic Fleet
Fleet Information Warfare Center Commander CAPT G. Barrett
ADDU
CINCPACFLT
CINCUSNAVEUR
USNAVCENT
Executive Officer CDR D. Shimp
Technical Director Mr. Dan Walters
OIC FIWC DET SAN DIEGO
OIC EWOPFAC CHESAPEAKE
ADMIN N1
INTEL N2
OPS N3
Supply & Facilities N4
Tactics & Operational Plans N5
Analysis & C4 Systems N6
C2W Augment & Training N7
Electronics Maintenance N8
IW/C2W Requirements & Programs N9
IW Defense C2 Protect Lab
LAN Administrator

Organization: Fleet Information Warfare Center

Senior Information Warfare Official:

CAPT G. A. Barrett, Commanding Officer

Information Warfare Points of Contact:

Dan Walters, Technical Director
Bill Jones, Analysis and C4 Systems Department Head
LCDR Dean Rich, C2 Protect Division Officer

On-Line Resources:

FIWC NAVCIRT Homepage: http://www.fiwc.navy.mil

Information Warfare Related Organizations, Missions and Functions:

The FIWC is the Navy's IW Center of Excellence. The FIWC is located at Little Creek Amphibious Base, VA with a detachment in San Diego, CA. FIWC missions include:

- Act as the Fleet CINC's principal agent for development of IW/C2W tactics, procedures, and training, under the operational control of Commander in Chief, U.S. Atlantic Fleet (CINCLANTFLT), additional duty to Commander in Chief, U.S. Pacific Fleet (CINCPACFLT), Commander in Chief, U.S. Naval Force Europe (CINCUSNAVEUR), and Commander, U.S. Naval Forces Central Command (CMUSNAVCENT). Deploy personnel trained in the IW/C2W disciplines of exploit, protect, and attach with appropriate counter-C2/C-2 protect hardware and software systems to support Battle Group and Joint Task Force operations.
- In coordination with the Fleet CINCs, Numbered Fleet Commander, and COMNAVDOCCOM, develop and disseminate integrated naval IW/C2W tactics, techniques, and procedures to Fleet units and shore support establishments worldwide.
- Coordinate naval IW/C2W tactics, procedures, and training with the joint centers and the other services' IW/C2W related centers.
- Maintain liaison with national agencies, other service centers, and the Naval Information Warfare Activity (NAVINFOWARACT) to facilitate satisfaction of IW/C2W related requirements submitted by the Fleet.
- Provide to the CNO, Fleet CINCs, COMNAVSECGRU, and NAVSYSCOMs advice, assistance, and recommendations on requirements and priorities for research and development, procurement, and training which supports IW/C2W applications.
- Provide IW/C2W protect teams to support operational and shore establishments.
- An Information Manager security officer will augment and deploy as part of each Battle Group's IW Commander's staff.

FIWC provides Navy operating forces and shore establishments with the following support:

- Deployable shipboard IW teams
- Offensive and defensive IW support
- Signals intelligence exploitation
- On-line computer surveys (Vulnerabilities)
- Computer Incident Response Team (Emergency Response)
- Train and equipment Battle Group Staffs (Training)

To support Defensive IW, FIWC provides the following services to support DoN information systems:

- Navy Computer Incident Response Team (NAVCIRT). Provides computer security and incident response capabilities for fleet and shore-base commands. Serves as the Navy's clearinghouse for knowledge and tools related to IW/C2W Protect.
- Vulnerability Analysis and Assessment Program. Provides DoN commands with an analysis of their computer networks to identify vulnerabilities. The VAAP operates SUN SPARC workstations, with the capability to conduct unclassified to Top Secret level assessments.
- Automated Security Incident Measurement (ASIM). Navy has initiated the use of ASIM on Battle Groups classified systems. The ASIM provides improved monitoring capability for the information system operator, and is laying the groundwork for a Navy-wide initiative to integrate monitoring, detection, isolation, and reaction capabilities into security architectures. ASIM recognizes attempts by unauthorized personnel to gain access to Navy networks, notifies appropriate personnel of the intrusion attempt, and automatically records the intrusion.

Information Warfare Activities, Issues, Best Practices, Lessons Learned:

- The FIWC hosts the IW/C2W lessons learned database.
- Results of On-Line Surveys have raised awareness at senior level regarding vulnerabilities to sensitive but unclassified systems, and classified systems built on COTS products.
- Navy has built strong working relationships with other Services and DISA CERT organizations, and has gone to great extent to share lessons learned and tools.
- Navy has conducted numerous follow-on assessments on behalf of organizations to determine improvements to systems security. These assessments have been integral to increased system administrator training and awareness.

Organization: Naval Information Warfare Activity

Senior Information Warfare Official:

CAPT T. Daly, Commanding Officer

Information Warfare Points of Contact:

LCDR R. Zellman

On-Line Resources:

Information Warfare Related Organizations, Missions and Functions:

The Naval Information Warfare Activity (NIWA) is headquartered at Fort Meade, MD, with subordinate organizations at the Naval Research Laboratory, Washington, DC, and the National Maritime Intelligence Center, Suitland, MD. The NIWA is the CNO's principal technical agent and interface to Navy and national Agencies pursuing information warfare technologies. In this role the NIWA acts as technical agent for development and acquisition of navy special technical capabilities supporting IW systems.

The NIWA also serves as the Navy's technical agent for appropriate simulation and modeling activities supporting IW.

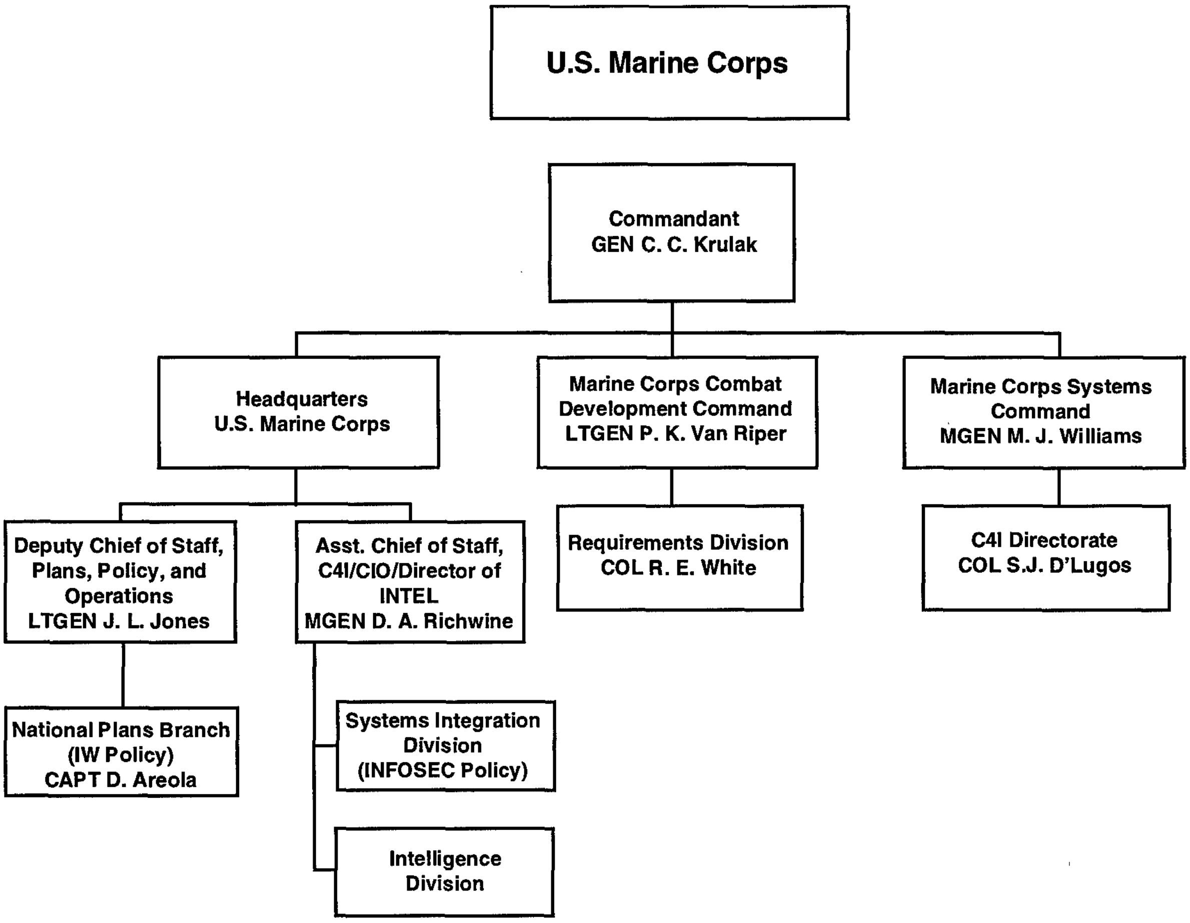
NIWA mission is to:

- Act as CNO's principal technical agent and interface to Service and national level agencies engaged in the pursuit of information warfare technologies.
- Conduct technical liaison with appropriate national agencies and provide resulting information warfare data/data bases to CNO (N6), COMNAVSECGRU, and the FIWC, et al.
- Conduct and/or manage all technical partnership activities with national-level agencies for technology development and IW applications and provide relevant IW data to CNO (N6), COMNAVSECGRU, FIWC, to support IW/C2W operations planning.
- Act as the principal technical interface with FIWC for transition of IW special technical capabilities for naval and Navy-supported joint operations.
- In accordance with current tasking, act as technical agent for development and acquisition of Navy special technical capabilities supporting IW systems.
- Conduct technical threat analysis and vulnerabilities assessment studies, develop technical requirements for, and evaluate/assess new information technologies, competitive architectures, and advanced concepts for offensive and defensive IW systems.

Information Warfare Activities, Issues, Best Practices, Lessons Learned:

- A key role of NIWA is to perform RF vulnerability assessments for developing Navy systems, i.e., satellite systems such as MILSAT, and INMARSAT. As IW initiatives have focused on networks and interconnectivity, NIWA is focusing on efforts to assess a "system of systems."
- NIWA is developing a better mechanism to identify information systems vulnerabilities in the conceptual or design phase. Further, NIWA is attempting to prioritize which critical systems demand vulnerability assessments.
- To increase the usefulness of vulnerability assessments, NIWA is developing a standard vulnerability assessment report that will be more meaningful to the acquisition community.
- The results of vulnerability assessments will be combined with more precise threat assessments, recommended countermeasures, and minimum risk guidance enabling the Program Manager to make objective risk management decision.

This page intentionally left blank.



U.S. Marine Corps

Commandant
GEN C. C. Krulak

Headquarters
U.S. Marine Corps

Marine Corps Combat
Development Command
LTGEN P. K. Van Riper

Marine Corps Systems
Command
MGEN M. J. Williams

Deputy Chief of Staff,
Plans, Policy, and
Operations
LTGEN J. L. Jones

Asst. Chief of Staff,
C4I/CIO/Director of
INTEL
MGEN D. A. Richwine

Requirements Division
COL R. E. White

C4I Directorate
COL S.J. D'Lugos

National Plans Branch
(IW Policy)
CAPT D. Areola

Systems Integration
Division
(INFOSEC Policy)

Intelligence
Division

Organization: United States Marine Corps

Senior Information Warfare Officials:

LtGen A. C. Blades, Deputy Chief of Staff for Policy, Plans, and Operations
MajGen D. Richwine, Assistant Chief of Staff for C4I/Director of Intelligence

Information Warfare Points of Contact:

Capt Dave Areola, National Plans Branch, ODCS for Policy, Plans, and Operations
Major Bob Wiedower, National Plans Branch, ODCS for Policy, Plans, and Operations
LtCol Marshall Snyder, Systems Integration Division, ACS, C4I

On-Line Resources:

U.S.M.C. Homepage: www.usmc.mil

Information Warfare Related Organizations, Missions and Functions:

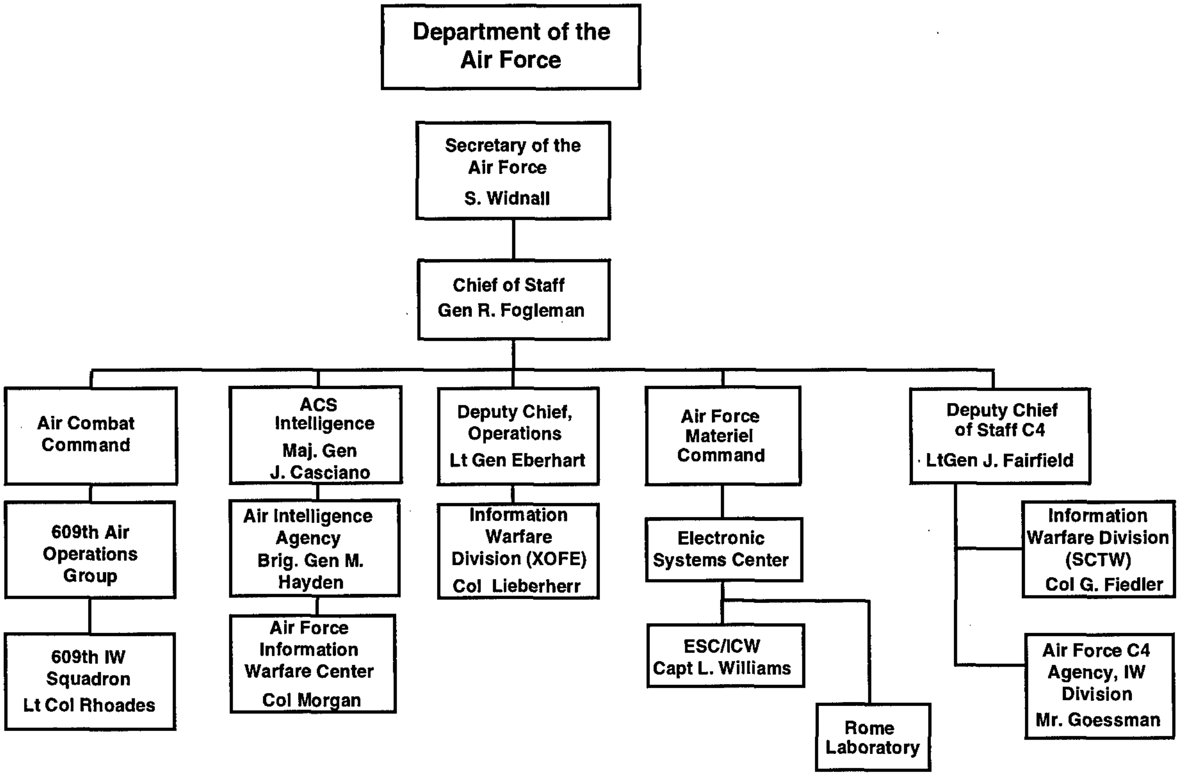
Headquarters, Marine Corps (HQMC) is responsible for IW-D policy. The National Plans Branch within the Plans, Policy and Operations Department, HQMC is responsible for IW and C2W policy. The C4I Department, HQMC is charged with INFOSEC and COMPUSEC policy. Combat Developments Command is responsible for requirements and Systems Command is responsible for development and acquisition.

Information Warfare Activities, Issues, Best Practices, Lessons Learned:

- HQMC issued Marine Corps Order 3430.5A, Policy for Command and Control Warfare (C2W). The Marine Corps is more comfortable with Command and Control Warfare than Information Warfare. C2W is better defined and oriented toward the tactical and operational levels of war and therefore more coincident with Marine Corps missions.
- A small force, the Marine Corps must leverage their funds and billets by taking advantage of Navy and other Service initiatives. For example, Marine billets in the FIWC, NIWA, the AFIWC, and the JC2WC, ensure they are "in the loop" and receive a share of the services provided by these organizations.
- Panels and Working Groups: HQMC has established an IW working group to coordinate IW activities between all HQMC departments, the Marine Corps Combat Development Command (MCCDC), and the operating forces.
- Protect: The Marine Corps is investigating ways to that COMSEC and C2W tools get down to the operating forces. Seventeen (17) firewalls are being implemented at the NIPRNET gateways to the USMC Banyan network.

- Detect and React: The Marine Corps is working with the FIWC; the home of the Navy Computer Incident Response Team, to receive emergency response support. The FIWC is scheduled to conduct on-line surveys, probes of Marine Corps networks and systems, this summer. The purpose of the survey is to establish a baseline of system vulnerabilities. Follow-up surveys are envisioned but on an as needed basis. Neither the Navy or Marine Corps plan to establish a Red Team organization.

This page intentionally left blank.


Department of the Air Force
Secretary of the Air Force S. Widnall
Chief of Staff Gen R. Fogleman
Air Combat Command
609th Air Operations Group
609th IW Squadron Lt Col Rhoades
ACS Intelligence Maj. Gen J. Casciano
Air Intelligence Agency Brig. Gen M. Hayden
Air Force Information Warfare Center Col Morgan
Deputy Chief, Operations Lt Gen Eberhart
Information Warfare Division (XOFE) Col Lieberherr
Air Force Materiel Command
Electronic Systems Center
ESC/ICW Capt L. Williams
Rome Laboratory
Deputy Chief of Staff C4 LtGen J. Fairfield
Information Warfare Division (SCTW) Col G. Fiedler
Air Force C4 Agency, IW Division Mr. Goessman

Organization: Department of the Air Force

Senior Information Warfare Officials:

Lt Gen Ralph Eberhart, Deputy Chief of Staff for Plans and Operations
Lt Gen John S. Fairfield, Deputy Chief of Staff for C4I
Maj Gen John P. Casciano, Assistant Chief of Staff for Intelligence

Information Warfare Points of Contact:

Col Lieberherr, Information Warfare Division (XOFE), Office of the Deputy Chief of Staff for Plans and Operations
Col George Fiedler, Chief, Information Warfare Division (SCTW), Office of the Deputy Chief of Staff for C4I
Lt Col Blunden, Special programs Division (INXI), Office of the Assistant Chief of Staff for Intelligence
Howard Schmidt/John DeMaggio, Air Force Office of Special Investigations
Goessman, Information Protection Division, Air Force C4 Agency
Capt Lee Williams, Information Warfare Division (ICW), Electronic Systems Center
Maria Ramirez, AIA/XPR, Air Intelligence Agency
Feliciano Rodriguez, Air Force Information Warfare Center
John Pirog, IWT, Rome Laboratory
Lt Col Rhoades, 609th IW Squadron

On-Line Resources:

USAF Homepage: http://www.dtic.mil:80/airforcelink/

Information Warfare Related Organizations, Missions and Functions:

Deputy Chief of Staff for Operations (XO): XO has the lead for coordinating information warfare doctrine in the Air Force. XO has established an Information Warfare Division (XOFE) that leads the Information Dominance Panel directing $4 Billion in Air Force programs.

Deputy Chief of Staff for Communications and Information (SC): SC is responsible for orchestrating Information Protection (IP) efforts across the Air Force and for ensuring that IW and IP are considered in all planning efforts. SC has established an Information Warfare Division (SCTW).

> Air Force C4 Agency (AFC4A): AFC4A is responsible for developing C4 security policy.

Electronic Systems Center (ESC): ESC has established an IW Division which is responsible for selection, installation and sustainment of Base Information Protection Products.

Rome Laboratory, ESC, is establishing a single, integrated, laboratory-wide science and technology thrust for information warfare.

The Air Force Information Warfare Center (AFIWC) was established, in October 1993. An organizational summary for the AFIWC follows.

609th IW Squadron: The 609th is a prototype Information Warfare Squadron at Shaw AFB. Deployable AFIWC-type services will be provided by IW Squadrons.

Air Force Office of Special Investigations (OSI): OSI has established a computer forensics laboratory at Bolling Air Force Base.

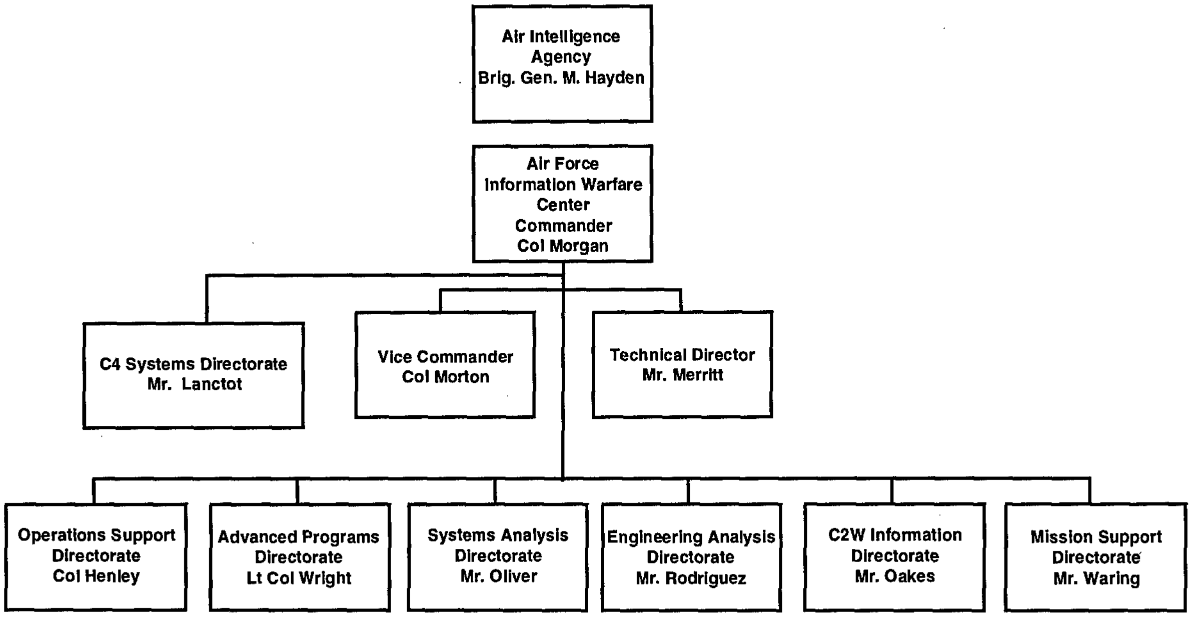
Due, in part, to the integrated, cross-cutting approach to IW within the Air Force, many line and staff organizations at various levels are actively involved integrating IW into Air Force doctrine, policy, plans, programs, and procedures. At the Air Staff, the operations, C4, intelligence, information management, acquisition, and security police communities participate in the Information Protection Working Group and other forums. Line organizations, such as the Air Force C4 Agency, Electronic Systems Command, the 38th EIW at Tinker AFB, and the Air Logistics Command in San Antonio are key contributors. MAJCOMs have assigned information protection (IP) responsibilities and Base Information Protection Offices have been established at the base level under Base Communications Squadrons.

Information Warfare Activities, Issues, Best Practices, Lessons Learned:

- *Cornerstones of Information Warfare,* released in Aug 95, provides the Air Force doctrinal foundation as a first step toward integrating information warfare into Air Force doctrine. The concepts in *Cornerstones* are being incorporated into Basic Air and Space Doctrine of the United States Air Force (AF Manual 1-1). *Cornerstones* uses airpower terminology and examples to describe IW and proposes new Air Force missions of Counterinformation, C2 Attack, and Information Operations. The White Paper, *Air Force Information Protection Vision* , dated 25 April 1995, identifies an Information Protection (IP) strategy. A series of Air Force Instructions (AFI 33-2 series), covering all aspects of IP, have recently been revised or are in the process of being revised. ESCs Base Information Master Plan and the BNCC CONOPS address IP at the base level.
- Panels and Working Groups: The Air Force Corporate Board structure--a hierarchy of executive panels and steering groups--and the IW Technical Planning Integration Process Team (IWTPIPT)are key to integrating IW into Air Force operations, functions and organizations. The IWTPIPT uses a cost constrained, 25 year modernization planning process. The IWTPIPT is co-chaired by ESC and AFIWC. Within the Air Force Corporate Board structure, the C4I Panel, chaired by SC, and the Information Dominance Panel, chaired by XOFE, are the principal panels addressing IW issues. The INFOSEC Program Element, which, among other things, funds the AFIWC, falls under the Information Dominance Panel. Another key group at the Air Staff level, is the Information Protection Working Group (IPWG). Members include representatives from the Assistant Chief of Staff for Intelligence (IN), XO, SC, and representatives from the acquisition, information management, and security police communities. The principal

responsibility of the IPWG is coordination of Air Force wide efforts to protect Air Force information and automated information systems and processes. Base Information Protection Working Groups and Information Infrastructure Steering Groups also contribute to protection of the base infrastructures.

- Risk Management: The Air Force is a strong proponent of a risk management approach to IW-D. Through vulnerability and threat assessments, a risk management process is employed to provide appropriate protection based on operational priorities while considering economies of scale. The Air Force Risk Management Model, developed by the AFIWC, has been proposed for adoption by OSD.
- Protect: The Combat Information Transport System (CITS) is a base infrastructure upgrade program which provides a fiber optic backbone, base switches, and funds the BNCCs and security requirements. The FY 97 POM provides for 60% funding of the infrastructure programs and 100% of the security requirement. Support to deployed forces will be provided by Deployed Network Control Centers (DNCC) with a second tier of support at the AFFOR level. The Air Force is beta testing FORTEZZA and Armor Mail and is pursuing a MLS enclave beta test for the SC staff.
- Detect and React: The Base Network Control Center (BNCC) is the focal point for base network management and protection. Security tools to do self assessments; e.g., on-line surveys, automated network management, intrusion detection capabilities, are planned for integration into the BNCC. The first step provides free or low cost tools the BNCCs to quickly provide some measure of IP. The BNCCs are provided integrated network management and IP support from MAJCOM Network Support Centers, the Air Force Network Support Center and the AFIWC. The Air Force is also pursuing increased coordination between the AFIWC and other Service and Agency IW activities such as the DISA ASSIST, Army's LIWA and the Navy's NIWA.
- Training, Education and Awareness: The Air Force feels that training provides the greatest return on investment in IP. A Process Action Team (PAT) is looking at all levels of training. Professional Military Education programs are underway for O-6's and Flag Officers. Network Management Training is provided by Air Education and Training (AETC) Command at Keesler AFB. An initiative is also underway to incorporate IP training at the unit level.
- Legal: The Air Force General Counsel has completed a report on IW legal issues. The final report is classified.


Air Intelligence Agency Brig. Gen. M. Hayden
Air Force Information Warfare Center Commander Col Morgan
C4 Systems Directorate Mr. Lanctot
Vice Commander Col Morton
Technical Director Mr. Merritt
Operations Support Directorate Col Henley
Advanced Programs Directorate Lt Col Wright
Systems Analysis Directorate Mr. Oliver
Engineering Analysis Directorate Mr. Rodriguez
C2W Information Directorate Mr. Oakes
Mission Support Directorate Mr. Waring

Organization: Air Force Information Warfare Center

Senior Information Warfare Officials:

Col Frank M. Morgan, Commander

Information Warfare Points of Contact:

Feliciano Rodriguez, Director, Engineering Analysis Directorate
Fred Ramirez, AFCERT

On-Line Resources:

AFIWC Homepage: http://www.aia.af.mil/hqaia/afiwc

Information Warfare Related Organizations, Missions and Functions:

AFIWC's mission is to develop, maintain, and deploy information warfare/command and control warfare (IW/C2W) capabilities in support of operations, campaign planning, acquisition, and testing. The Center acts as the time-sensitive, single focal point for intelligence data and C2W services. It provides technical expertise for computer and communications security (COMPUSEC/COMSEC) and is the Air Force's focal point for tactical deception (TD) and OPSEC training.

The Engineering Analysis (EA) Directorate supports information and weapon systems development by providing technical guidance in the areas of computer and communications security; supports Information Protect (IP) through management of the C4 Systems Security Assessment Program (CSAP) to improve the security posture of AF C4 systems; develops security countermeasures, specialized tools and provides security engineering consultant services; manages and operates the Air Force Computer Emergency Response Team (AFCERT); and serves as the C4 systems security technical office for IP product and field assessments, security test and evaluation, electromagnetic field and lab emission security and zone testing.

The Air Force Computer Emergency Response Team (AFCERT) was established by the Air Force Information Warfare Center as the single point of contact in the Air Force for reporting and handling computer security incidents and vulnerabilities. The AFCERT coordinates the technical resources of AFIWC to assess, analyze, and provide countermeasures for computer security incidents and vulnerabilities reported by Air Force computer users, security managers, and system managers. The AFCERT deploys incident response teams to recover networked computer systems under attack from unauthorized sources. AFCERT Advisories are furnished to all users providing the latest information on system vulnerabilities and applicable countermeasures. The AFCERT coordinates computer security-related activities with all outside agencies and provides technical support to the Air Force Office of Special Investigations (AFOSI) during criminal and counter-intelligence investigations.

The Countermeasures Engineering Team (CMET) is responsible for integrating and validating technical computer and network security solutions for identified operational security vulnerabilities. The CMET's technical successes experienced through the development of intrusion detection tools, e.g., DIDS and NSM, vulnerability testing techniques, e.g., OLS, and specialized support to the AFCERT's incident response and recovery operations, were due in large part to the research and countermeasure prototype activities analogous with CMET operations. The CMET also provides engineering expertise to the telephone switch vulnerability assessment program and identifies countermeasure solutions. The continued operation of the CMET allows quick corrective reaction to new vulnerabilities identified during AFCERT operations.

The Electronic Security Survey Team (ESST) is a key component of the Air Force Information Warfare Center's Command, Control, Communications, and Computer (C4) Systems Security Assessment Program (CSAP). The major objective of the ESST is to improve C4 systems security posture by measuring the effectiveness of organizational electronic security and recommending COMSEC, COMPUSEC, and TEMPEST countermeasures where deficiencies exist. The 67 Intelligence Wing (67IW) deploys ESSTs to conduct Electronic Security Surveys (ESSs) for Air Force commanders worldwide. The ESST performs a field assessment to measure and evaluate the current computer, communications, and TEMPEST security posture of an Air Force facility. ESS assessments are accomplished in two phases: low profile and high profile. During the low-profile phase, a physical evaluation of individual work stations is conducted. The focus of this phase is to find unauthorized software, passwords, review magnetic media labeling, unauthorized connectivity, and search for obvious computer security vulnerabilities. The purpose of the high-profile phase is to identify procedural vulnerabilities and gauge the level of C4 system awareness and training of assigned members. Identified vulnerabilities, recommended countermeasures, and a local area threat study are presented in the final report.

The Electronic Security Engineering Team (ESET) performs field surveys to measure and evaluate the current C4 system security posture of Air Force facilities. The survey teams identify technical vulnerabilities and recommend solutions. Engineering teams use a variety of automated security tools. These tools include: anti-virus products, Computer Oracle and Password System (COPS), password cracking tools, firewalls to block certain traffic to a protected network, Internet Security Scanner (ISS), Network Security Monitor (NSM), Security Profile Inspector (SPI), TCP Wrappers to monitor incoming network traffic, and TRIPWIRE to monitor a designated set of files for changes.

Security Technology Insertion and Test Team (STIT) provide technical support to MAJCOMs, SPOs, AFOTEC and field units for security solution, weapon system and C4I system development and test efforts. The STIT Teams will: (1) develop, test, and integrate security solutions for security deficiencies; (2) perform security product testing in support of solutions and customer requests (3) analyze new operating systems being used in new/upgraded weapon and C4I systems; and (4) perform vulnerability testing in support of security test and evaluation of acquisition/upgrade program efforts.

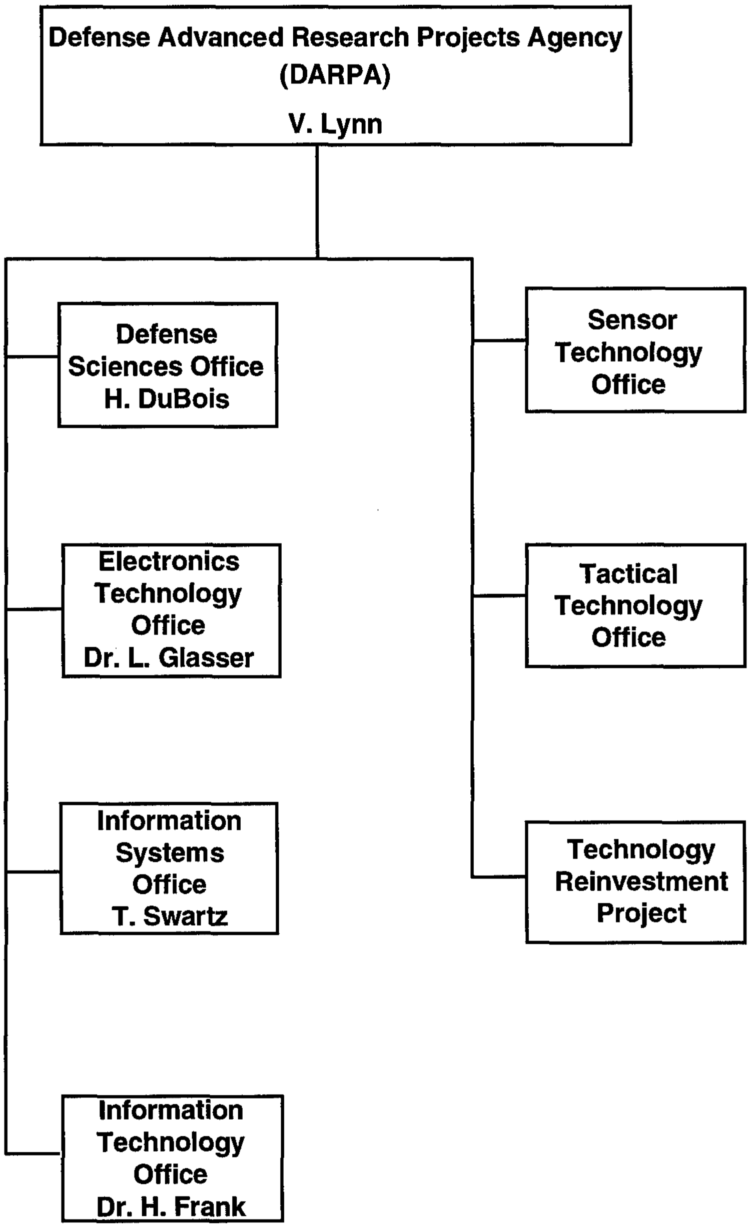
- A solution development team identifies solutions for documented security deficiencies in customers' networks. This team provides recommendations as well as prototyping and integration of solutions at customer site and/or in the EA technology LAB. This team assists in the development of secure network architectures for identified security deficiencies.
- Security product testing includes conducting product assessments in support of solution development, individual customer requests, or under direction from the Air Staff or AFC4A. Product testing includes functional security tests, vulnerability testing, and identification of security integration issues associated with the security products.
- Analysis of new/upgraded weapon and C4I systems that will be deployed within the Air Force and key operational systems. Analysis includes testing for existing security vulnerabilities, security weaknesses, and associated risks of fielding the operating systems within weapon and C4I systems with specific configurations and applications.
- Engineering teams assist SPOs, FOTEC, and other organizations with the conduct of ST&Es for specialized AF systems. This assistance will be for the specific purpose of performing vulnerability testing in support of security test and evaluation of acquisition/upgrade program efforts.

Information Warfare Activities, Issues, Best Practices, Lessons Learned:

- The AFCERT conducts On-Line Surveys (OLS) to measure the security posture of Air Force Systems. Survey operators attempt to penetrate targeted systems using known vulnerabilities. These penetration attempts should be detected by system administrators and reported to the Air Force Computer Emergency Response Team (AFCERT). The OLS team analyzes all data generated from testing and creates a report. This report is distributed to the base commander of the targeted systems and the MAJCOM. The report describes the security weaknesses found on each system targeted and the associated countermeasure. The report also tells where the administrator needs to go for further information and help. The OLS results are used to steer Air Force efforts to strengthen Air Force C4 systems security.
- The Network Security Monitor (NSM) Program is designed to measure the level of unauthorized activity against Air Force C4 systems. The network traffic data from individual sites is reported to and centrally analyzed by the AFCERT every 24 hours. NSM analysts then measure the level of unauthorized activity using a Statistical Process Control (SPC) methodology. When network traffic analysis reveals suspected unauthorized activity using a Statistical Process Control (SPC) methodology. When network traffic analysis reveals suspected unauthorized activity, the AFCERT validates the data with the affected unit and initiates incident response measures. The AFOSI is informed and opens an investigation at the NSM site as appropriate. The AFOSI may request technical assistance from the AFCERT to support their investigation. NSM is currently operational at 38 sites and is approved for Air Force-wide installation by December 1997. There are two main areas of future development for NSM. First, portability to Linus-based personal computers and second, increasing user-friendliness of NSM's graphical interface with real-time data.

- The AFCERT manages the C4 Database System (CDS) that provides for complete documentation of Air Force computer security incidents, virus profiles, countermeasures, vulnerability testing, and network monitoring activities. The CDS affords the AFCERT on-line access to computer security statistical data that provides the security posture of networked computer systems Air Force wide. Future development includes CDS on-line access by AF Major Commands and Base Network Control Centers (BNCC).
- The Distributed Intrusion Detection System (DIDS) is designed to identify and report misuse of computer systems. It does so by tracking users, finding out where users are coming from, what they are doing, and looking for known patterns of misuse. It is designed as a tool to assist network administrators or Computer Systems Security Officers (CSSOs) in maintaining the security of their systems. DIDS provides the ability to track users across the network using the Network ID (NID). It identifies users despite changes in login names and remote logins to other computers and provides the network administrator or CSSO centralized access to network information about the security status of a system. The DIDS Director is the central computer which correlates the information it receives and produces human-readable reports for the CSSO. Each monitored host runs a host monitor which collects and analyzes audit records from the operating system. It looks for notable security-related events and sends them to the DIDS Director for further analysis. Future development includes a hierarchical DIDS Director to monitor wide area networks.
- The Information Protect Operations Decision Support System (IPODSS) is a new concept developed by the AFIWC that provides for the collection, integration and display of threat, vulnerability, and system data that will be used to quantify risks and develop courses of action (COAs) for Information Protection (IP) operations. Specifically, IPODSS will provide continuous status of IP posture, integrate indications and warning (I&W) support, and near-real-time (NRT) analysis and decision support for IP operations. Providing continuous status of the IP posture means monitoring and displaying system connectivity, vulnerability, threat, and performance data in NRT. The status of deployed and deployable IP assets (e.g., incident response teams) also should be monitored. IPODSS should be capable of distilling these data into overall assessments of the risk posture within an area of interest. Integrated I&W support means analyzing and correlating traditional and network-derived intelligence to facilitate more timely assessments of adversary intent and allow for prompt dissemination of appropriate warning and action messages. Traditional I&W includes detection of force deployments, increased communications, etc. Network-derived intelligence includes detections of system intrusions, assessments of likely targeted systems, etc. IPODSS should be capable of accessing and analyzing both structured and unstructured threat data (from traditional and emerging sources) to support timely I&W. The resulting assessments will be disseminated, along with directed COAs formulated via the analysis and decision support capabilities of IPODSS. Full realization of IPODSS analysis and decision support capabilities will require development and implementation of integrated operations centers. In the integrated operations center, data should be fused and correlated to support graphical display of the IO situation in operator-selectable regions. The decision support capabilities of the system should then allow rapid assessment of options (e.g., via sim/mod applications) to provide insight into projected outcomes. Intermediate analysis inputs,

situation tracks, responsive capabilities, and other operational data also should be available. Multi-function displays (MFDs) should be used to allow flexible, configurable display of operator-selected information. The IPODSS initiative is currently being coordinated with other Air Force and DoD agencies.


Defense Advanced Research Projects Agency
(DARPA)
V. Lynn
Defense Sciences Office
H. DuBois
Electronics Technology Office
Dr. L. Glasser
Information Systems Office
T. Swartz
Information Technology Office
Dr. H. Frank
Sensor Technology Office
Tactical Technology Office
Technology Reinvestment Project

Organization: Defense Advanced Research Projects Agency

Senior Information Warfare Official:

Dr. Howard Frank, Director, Information Technology Office, DARPA

Information Warfare Points of Contact:

Ms. Teresa Lunt, Program Manager, ITO, DARPA

On-Line Resources:

DARPA Homepage: http://www.darpa.mil/
DARPA Information Survivability Homepage:
http://www.ito.darpa.mil/ResearchAreas/Information_Survivability.html

Information Warfare Related Organizations, Missions and Functions:

DARPA is responsible for advanced research in areas related to Defensive Information Warfare.

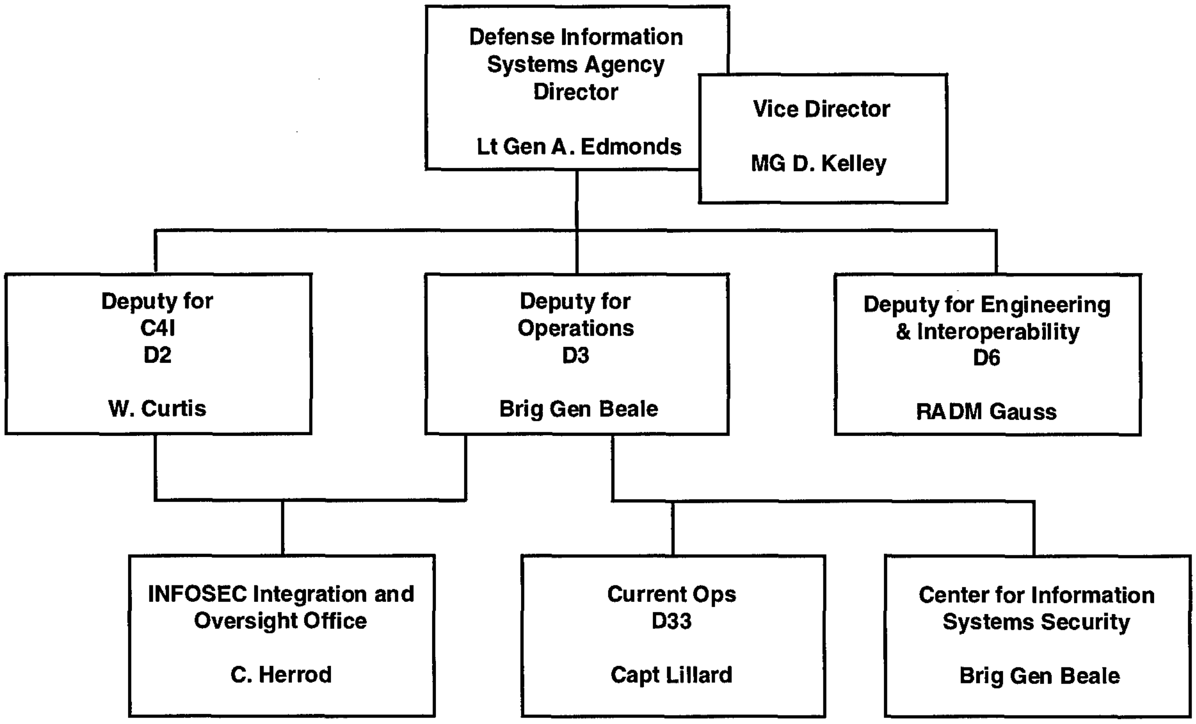
Information Warfare Activities, Issues, Best Practices, Lessons Learned:

- DARPA is a co-founder, with DISA and NSA, of the Information System Security Research Joint Technology Office (ISSR-JTO). The ISSR-JTO was established to coordinate the information systems security research programs of DARPA and NSA. The ISSR-JTO works to optimize use of the limited research funds available, and strengthen the responsiveness of the programs to DISA, expediting delivery of technologies that meet DISA's requirements to safeguard the confidentiality, integrity, authenticity, and availability of data in DoD information systems, provide a robust first line of defense for IW-D, and permit electronic commerce between the DoD and its contractors.
- DARPA has renamed its Defensive Information Warfare program to Information Survivability. The Information Survivability program creates advanced technologies to protect DoD's mission-critical capabilities against electronic attack upon or through their supporting computing infrastructure. The goal is to create affordable, verifiable, scaleable technologies for a robust and secure defense infrastructure through configurable replaceable components and robust system design technology.
- The focus of the Information Survivability program is in the following four areas:
  - High Confidence Networking: Interoperable, scaleable, verifiable protocols and network security services to provide security and reliability to higher-level applications.
  - High Confidence Computing Systems: Modular, verifiable prototype systems with configurable replaceable components for security, reliability and real-time.
  - Assurance and Integration: Tools for designing, integrating and evaluating systems for security and robustness.

- Survivability for Large Scale Information Systems: Techniques and tools to achieve survivability of large-scale defense infrastructure systems

- In 1995 DARPA sponsored a IW-D Summer Study to examine whether the nation's critical information infrastructure could be hardened to improve survivability against a wide range of possible threats. The following is a brief summary of the study's findings.
  - The systems that matter are often complex, unstructured, and include COTS and legacy components.
  - The process of hardening complex systems is poorly understood.
  - Laboratory successes are not impacting the nationally critical technologies.
  - The requirement: a practical technology for selectively hardening complex systems to achieve "high confidence" solutions.
- Robustness of systems must be widely defined. Two useful models can be found in biological and social systems. For example, a public health infrastructure could be created to immunize the population, and diversity would ensure that a population is not susceptible to a single attack.

This page intentionally left blank.


Defense Information Systems Agency Director
Lt Gen A. Edmonds
Vice Director
MG D. Kelley
Deputy for C4I D2
W. Curtis
Deputy for Operations D3
Brig Gen Beale
Deputy for Engineering & Interoperability D6
RADM Gauss
INFOSEC Integration and Oversight Office
C. Herrod
Current Ops D33
Capt Lillard
Center for Information Systems Security
Brig Gen Beale

Organization: Defense Information Systems Agency (DISA)

Senior Information Assurance Official:

Lt Gen Al Edmonds, Director, DISA

Information Assurance Points of Contact:

Brig Gen James Beale, USAF, Deputy Director for Operations (D3)
Chrisan Herrod, Chief, INFOSEC Integration and Oversight Office, Directorate of Operations (D3)
Sara Jane League, Deputy Director, Center for Information Systems Security (CISS)

On-Line Resources:

DISA Homepage: http://www.disa.mil/
DISA CISS Homepage: http://www.disa.mil/ciss/index.html

Information Assurance Related Organizations, Missions and Functions:

DISA's IW-D responsibilities are those specified by directives and those implied by DISA's responsibilities to centrally manage the DII. The following directives outline the specific responsibilities:

- Department of Defense Directive 3222.4, Electronic Warfare (EW) and Command and Control and Communications Countermeasures (C3CM), July 31, 1992, which charged the Director, DISA, to "... ensure that DISA architectures consider EW, ECCM, and C3CM."

- Department of Defense Directive 8000.1, Defense Information Management Program, October 27, 1992, which tasked the Director, DISA, to "... in consultation with the Directors of the Defense Intelligence Agency and the National Security Agency, provide technology and services to ensure the availability, reliability and maintainability, integrity, and security of defense information, commensurate with its intended use."

- Department of Defense Directive TS 3600.1, Information Warfare, December 21, 1992, which assigned responsibility to the Director, DISA, to "... ensure the DII contains adequate protection against attack."

- Chairman of the Joint Chiefs of Staff Memorandum of Policy (MOP) Number 30, Command and Control Warfare, 8 March 1993, which tasked the Director, DISA, to "... assess the vulnerabilities of ... defense information systems..." and to "maintain procedures to ensure a capability to respond to identified threats and assessed vulnerabilities."

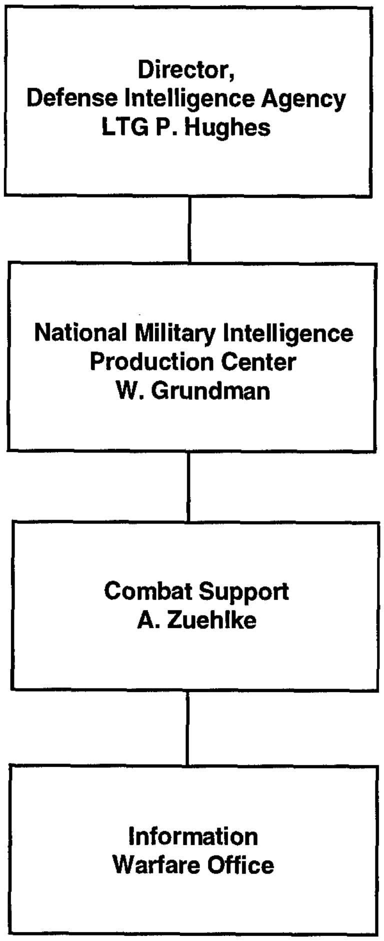
Formed in March 1996, the INFOSEC Integration and Oversight Office is jointly staffed by D2 and D3 with the function of overseeing the implementation of the DISA IW-D Management Plan, published 23 May 1996. The office will also develop the DoD IW-D Management Plan, assess the DII IW-D program, define DII protect, detect and react capability requirements, and develop performance goals and indicators and identify output measures for any assigned task.

DISA Center for Information Systems Security (CISS): The Center for INFOSEC (CISS), created by a Memorandum of Agreement between DISA and NSA on 12 May 1993, has the mission to develop and implement a Defense Information Warfare Program. The CISS is jointly manned by DISA and NSA personnel, in order to provide close coordination between the INFOSEC development and DoD implementor. The center was established as a DISA Field Operating Agency to support DoD, Joint and Service programs as required by DMRD 918 and to execute the Defense Information Systems Security Program (DISSP). To accomplish these key functions, CISS provides operational protection, detection, reaction and vulnerability analysis in support of the Defense Information Infrastructure; executes DoD requirements and processes for accreditation of computers, systems and networks; and develops, coordinates, and executes a DoD- wide INFOWAR education, training, and awareness program. CISS is also responsible for managing the INFOSEC Technical Services Contract and the DoD-wide Antivirus Software Initiative.

Information Assurance Activities, Issues, Best Practices, Lessons Learned:

- In its simplest form, the DISA strategy for achieving a secure DII is based on three security pillars: protect the DII components and information from intrusions and disruptions (malicious and other); detect the intrusions and disruptions when they occur; and, react to intrusions and disruptions of the DII. The react capability will include the ability to: differentiate among malicious and other disruptions; warn the appropriate operators and users of the disruptions; isolate affected infrastructure components; reallocate infrastructure capabilities; and, recover and reconstitute the DII capability.
- The DISA Defensive Information Warfare (IW-D) Management Plan published on 23 May 1996, outlines the steps the Director, DISA will undertake to ensure the DISA-owned and managed and the DISA-managed portions of the DII are adequately protected against attack.
- DISA is currently working on obtaining the following capabilities for the DII:
  - Integrated network management and security management
  - Audit Monitoring and Detection System (AMIDS)
  - Malicious Code Detection Eradication System (MCDES)
  - Automated Infrastructure Management System (AIMS)
  - Vulnerability Analysis and Assessment Program (VAAP)
  - Integrated Security Operation Capability for the DII GCC/RCC
  - Personnel, Training, and Facilities
  - Wargames and Exercises
  - Reserve Component Utilization

- DISA is a co-founder, with DARPA and NSA, of the Information System Security Research Joint Technology Office (ISSR-JTO). The ISSR-JTO was established to coordinate the information systems security research programs of DARPA and NSA. The ISSR-JTO works to optimize use of the limited research funds available, and strengthen the responsiveness of the programs to DISA, expediting delivery of technologies that meet DISA's requirements to safeguard the confidentiality, integrity, authenticity, and availability of data in DoD information systems, provide a robust first line of defense for IW-D, and permit electronic commerce between the DoD and its contractors.
- The Special Budget Issue (SBI) on Information Systems Security (INFOSEC) approved by the Defense Resources Board (DRB) on September 19, 1995, and documented in Program Decision Memorandum (PDM) II provided significant funding for protecting the DII.
- The INFOSEC Technical Services Contract was awarded in July 1995. It is a five year, indefinite-delivery, indefinite-quantity contract which will provide INFOSEC services and products for the Federal government.


Director,
Defense Intelligence Agency
LTG P. Hughes
National Military Intelligence
Production Center
W. Grundman
Combat Support
A. Zuehlke
Information
Warfare Office

Organization: Defense Intelligence Agency (DIA)

Senior Information Warfare Official:

Arthur Zuehlke, Director, Directorate for Combat Support, National Military Intelligence Production Center

Information Warfare Points of Contact:

Michael Lamb, Information Warfare Office
Dr. John Yurechko, Information Warfare Office
Glenn Price, Information Warfare Office

On-Line Resources:

DIA Homepage: http://www.dia.mil

Information Warfare Related Missions and Functions:

Manage the Defense intelligence community production to support the full range of DoD information warfare activities.

Serve as the Defense intelligence community focal point for the development, management, and maintenance of information warfare data bases that facilitate timely dissemination of all-source, finished intelligence in support of DoD information warfare activities.

Oversee DoD requirements, and serve as the Defense intelligence community focal point, for the development, management, and maintenance of information systems that facilitate timely collection, processing, and dissemination of all-source finished intelligence for DoD information warfare activities.

As DoD human intelligence (HUMINT) manager, provide oversight, guidance, and direction to the Defense HUMINT service, consistent with DoD information warfare objectives.

Oversee management of DoD intelligence information systems to ensure information warfare-related security requirements are defined and implemented.

Assist Unified Combatant Commands with the development of command intelligence architecture planning programs that fully integrate information warfare support requirements.

Assist the Chairman of the Joint Chiefs of Staff in developing joint information warfare doctrine and tactics, techniques, and procedures.

Coordinate with the DoD Components to share information warfare techniques and information warfare-related intelligence.

Oversee the cost-effective development of select information models and simulations foe scenario development, training and exercises, and targeting; and incorporate information warfare functions in the overall command, control, communications, computers and intelligence functional model.

Provide the Chairman of the Joint Chiefs of Staff and the Unified Combatant Commands with the timely intelligence required for effective information warfare target selection and post-strike analysis.

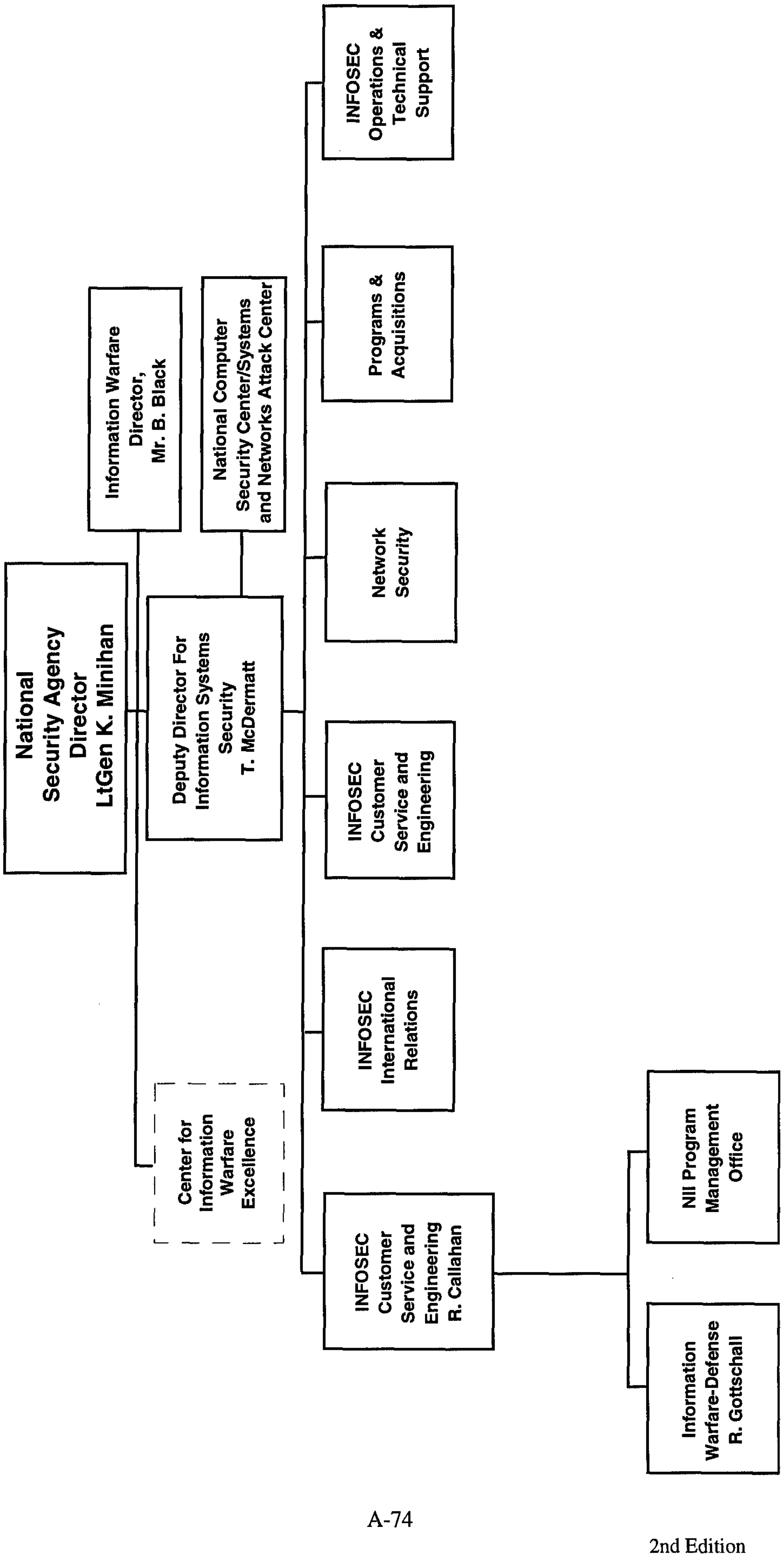
The DIA National Military Intelligence Systems Center is responsible for the certification and accreditation of DoD intelligence information systems and networks (excluding NSA systems).

DIA is responsible for development of foreign science and technology intelligence. In this role, DIA develops a strong awareness of foreign technology developments and transfers which could impact U.S. assets and capabilities.

Information Warfare Activities, Issues, Best Practices, Lessons Learned:

- DIA has established an Information Warfare Office with a staffing level of 135 people.
- DIA is currently leading four key intelligence efforts:
  - With the advent of the information age and the threat posed by information warfare, the U.S. intelligence community must adopt a new approach to fulfilling its strategic and tactical indications and warning responsibilities, Conventional indications and warning mechanisms, procedures, and protocols may not suffice for information warfare. DIA, responsible for providing indications and warning of foreign military attacks against the U.S. and its interests, is leading a U.S. government-wide effort to ensure the challenges presented by information warfare are met fully by both the DoD and the National Indications and Warning Communities.
  - DIA chairs a U.S. government-wide forum, the Interdepartmental Information Warfare Threat Working Group, to exchange and discuss relevant threat information.
  - DIA has also established the Information Warfare Working Group to define a process and procedures for the coordination and production of threat assessments for information warfare-related activities.
  - DIA is developing an Information Warfare Support System (IWSS) to permit the complete integration of all Defense Intelligence Community IW-related software programs and serve as a single source of IW intelligence throughout the globe for producers and consumers alike.

This page intentionally left blank.


National Security Agency Director LtGen K. Minihan
Information Warfare Director, Mr. B. Black
Deputy Director For Information Systems Security T. McDermatt
National Computer Security Center/Systems and Networks Attack Center
Center for Information Warfare Excellence
INFOSEC Customer Service and Engineering R. Callahan
INFOSEC International Relations
INFOSEC Customer Service and Engineering
Network Security
Programs & Acquisitions
INFOSEC Operations & Technical Support
Information Warfare-Defense R. Gottschall
NII Program Management Office

Organization: National Security Agency

Senior Information Warfare Official:

Bill Black, Director of Information Warfare

Information Warfare Points of Contact and Areas of Interest:

Dr. Clint Brooks, Information Strategy

On-Line Resources:

NSA Homepage: http://www.nsa.gov:8080/

Information Warfare Related Missions and Functions:

The Director of Information Warfare reports to the Director, NSA for Information Warfare issues. He has broad coordination responsibilities to monitor Information Warfare-related activities in both DoD and non-DoD government departments and agencies. He represents the interests of NSA across the entire spectrum of functional disciplines which impact on Information Warfare.

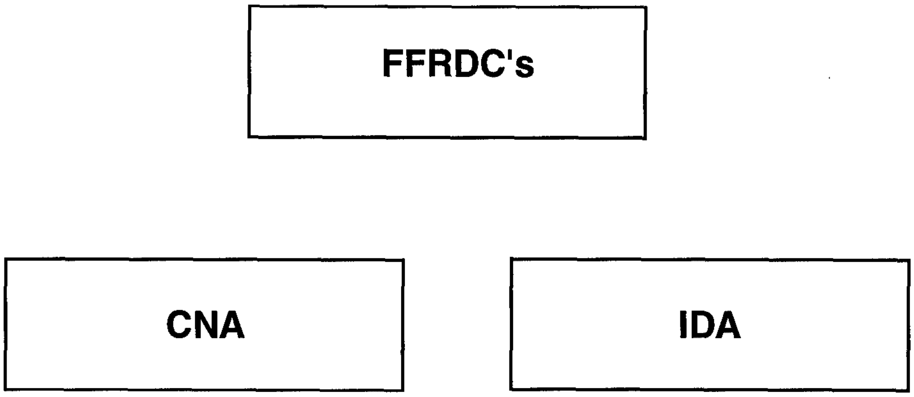
Information Warfare Activities, Issues, Best Practices, Lessons Learned:

- Defensive information warfare or information assurance activities are not yet well defined. The lack of definition is nowhere more apparent (in NSA's eyes) than when viewed through the Computer Security Act of 1987 (P.L. 100-235). The Act stipulates (in part) that government classified information systems-based data is the responsibility of NSA, while government unclassified information is the responsibility of NIST. The difficulty arises when one considers that 95+% of (classified or unclassified) communications is transmitted across public switches, and the quantity of computers which are in the public domain.
- NSA has developed a concept through which NSA will respond to issues of personal privacy, business privacy, law enforcement, and foreign intelligence with its well-founded systems security expertise. An example of an initiative being promoted to address these issues is the key escrow concept.
- The legal ramifications of IW are significant. On the offensive side, roles are fairly clear after the beginning of hostilities. Before hostilities, deconfliction is a big issue. On the defensive side, P.L. 100-235 is a big issue. What constitutes computer crime? Legal issues at the national level are murky at best. On the international level, it gets murkier.
- NSA responsibilities include SIGINT, INFOSEC, and OPSEC.
- There is a Professional OPSEC Society which promotes OPSEC in the private sector.
- The National Computer Security Center and the Information Systems Security Organization provide a variety of products and services to DoD and the Federal government. Services include threat analysis, research and technology development,

system security assessments and evaluations and system security engineering. Products include a variety of items being developed under the Multilevel Information Systems Security Initiative (MISSI) program.

- The National Computer Security Center is working in conjunction with the National Institute of Standards and Technology and several other nations (among them Canada, France, Germany, and the Netherlands) to develop a new set of guidelines called the Common Criteria. It is hoped by NSA and NIST that the Common Criteria will eventually replace the Orange Book (i.e., Trusted Computer Systems Evaluation Criteria).
- A Systems and Networks Attack Center (SNAC) was formed in May 1995 to replace portions of the National Computer Security Center. This center identifies systems and network vulnerabilities and network attack technologies.
- NSA has integrated the Information Systems Security Organization mission into the National Security Operations Center.
- NSA is in the process of establishing an Information Warfare Center of Excellence. This center will be jointly staffed by NSA, DIA, CIA, and others. It will focus on threats, vulnerabilities, and indications and warning.
- NSA is focused on the Global Information Infrastructure.

This page intentionally left blank.



FFRDC's

CNA

IDA

Organization: Center for Naval Analyses (CNA)

Senior Information Warfare Officials:

Ambassador Linton F. Brooks, Vice President, Policy Strategic Forces Division

Information Warfare Point of Contact:

Dr. Gary A. Federici

On-Line Resources:

Information Warfare Related Organizations, Missions and Functions:

CNA is a federally funded research and development center (FFRDC) serving as a center of inquiry for its sponsor, the Department of Navy. As an independent source of applied research and policy analysis, CNA assists senior leaders of the U.S. Navy and Marine Corps by conducting a continuing program of objective analysis and practical evaluations of naval operations, systems, and programs. CNA conducts analyses for other government organizations when the research is directly related to CNA's purpose, mission, and areas of expertise. For information warfare, CNA has focused on the following issues: (1) the key information warfare roles likely to be entrusted to the Navy; (2) what the Navy must do to adequately prepare itself to perform those roles; (3) how the future defense environment, including operations other than war, should drive the Navy's approach to information warfare; (4) evaluation of alternative information architecture that will support future operating forces; and (5) JWCA analytical support to the Joint Staff (J38/J6K).

Information Warfare Activities, Issues, Best Practices, Lessons Learned:

- CNA has conducted:
  - Evaluations of the role Information Operations and Warfare plays in joint training exercises.
  - Concept demonstrations of new approaches to using information systems in combat environments.
  - Classified IW technology evaluations.
  - Studies of service roles and missions.
- Key issues addressed were:
  - Approaches to defensive appliqués concept.
  - Peacetime planning for executing IW.
  - Approach to quantify contributions of IW.
  - Roles, missions, and functions.
  - National IW policy issues: gaps and opportunities.
  - Mission planning and organizing for IW.
  - Intelligence support to IW.

- CNA approaches all analytical issues by using empirical data, when possible. No modeling and simulations technology are employed. Field demonstrations and interaction with operations are the norm.
- Lessons learned are available through CNA points of contact.

Organization: Institute for Defense Analyses (IDA)

Senior Information Warfare Official:

Information Warfare Points of Contact:

Terry Mayfield, Computer Software and Engineering Division
Bill Barlow, Systems Engineering Division
Robert Anthony, Operational Evaluation Division

On-Line Resources:

IDA Homepage: http://www.ida.org/

Information Warfare Related Missions and Functions:

DoD Studies and Analyses

Information Warfare Activities, Issues, Best Practices, Lessons Learned:

- In 1995, DARPA sponsored a IW-D Summer Study to examine whether the nation's critical information infrastructure could be hardened to improve survivability against a wide range of possible threats. IDA contributed to this study. The following is a brief summary of the study's findings.
  - The systems that matter are often complex, unstructured, and include COTS components.
  - The process of hardening complex systems is poorly understood.
  - Laboratory successes are not impacting the nationally critical technologies.
  - The requirement: a practical technology for selectively hardening complex systems to achieve "high confidence" solutions.
- As a part of its Joint Warfare Capability Assessment of Information Warfare, the Joint Staff (J6K) requested the Institute for Defense Analyses (IDA) to research, analyze, and evaluate open systems technologies within the DoD and private industry to baseline IW technology. The results of that effort are documented in IDA Document D-1792, *Information Warfare Technologies: Survey of Selected Civil Sector Activities*, February 1996, and IDA Paper P-3157, *Information Warfare: Selected Long-Range Technology Applications*, February 1996.
- The IDA Document identifies 56 technologies with potential information warfare application and for each technology describes the technology strengths and weaknesses, possible concepts of operation, potential risks and related information such as technology availability, points of contact, and patent or proprietary aspects
- Three IDA organizations support IW-related activities, the Systems Engineering Division, Operational Evaluation Division, and the Computer and Software Engineering Division.

- IDA has been asked by J6K to address the role and impact of industry in defensive information warfare. They will also research technologies in or out of DoD which have potential application information warfare.
- IW-related activities include:
  - Supported JS/J38 in concepts development leading to CJCS MOP 30, Command and Control Warfare.
  - Analysis of counter-drug operations and security policy development and labeling of information to control dissemination of the counter-drug information.
  - Estimating value of information and cost of security within DoD. Currently attempting to extend approach to estimate cost of security in private sector.
  - Ten years supporting NSA in developing trusted computer systems evaluation criteria and evaluating commercial products against such criteria.
  - Drafted distributed systems functional evaluation criteria for NSA.
  - Developed security labeling analysis for DoD Common Security Label standard which supports network operations. Counter-drug operational experience was used to add realism to the standard.
  - Drafted study of baselining and implications of DoD Goal Security Architecture.
  - Assistance to NSA in drafting, review, and editing of the entire Rainbow series of documents.
    - Studying viability of DGSA concepts in commercial operating systems.
    - Studying viability of wrapper concept in Systems Security Architecture.
    - Provided distributed systems portions to Common Criteria (CC); Drafting Protection Profiles for use in evaluating CC.
  - Assisting NSA in revitalizing INFOSEC Education, Training, and Research Programs.
  - Synthesized integrity aspects of INFOSEC into NCSC Technical Reports 79-91 and 101-91.
  - In cooperation with NSA and the U.S. Naval Postgraduate School, IDA is establishing a Center of Excellence for Information Security. USNPGS point of contact is Dr. Cynthia Irvine.
  - Supported NSA and DISA in developing harmonized certification and accreditation procedures for DoD information systems.
  - Supported DISA in developing the DoD Goal Security Architecture (DGSA) which identifies where to establish security and the supporting rationale, and in developing the DGSA Overall Transition Strategy which integrates security functions identified in the DGSA and organizational responsibilities.
  - Provided support to DISA Center for Standards on DGSA Transition Activities involving Standards.
  - Assisted DARPA is developing a BAA on Information Security (95-15) and in evaluating the proposals. Approximately 150 proposals were received for the program which begins in FY 96 and will continue for three years. This program will address protection of operating systems, firewalls, intrusion detection, infrastructure protocols, infrastructure vulnerabilities, cryptography, and assurance tools and techniques.

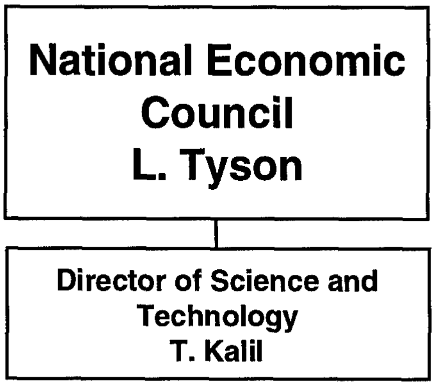
  - Assisted DARPA in developing a BAA for Information Survivability (BAA 96-03) which addresses technologies for a robust information infrastructure (consistency, distributed monitoring, staging of levels of protection, etc.).
  - Supported Office of Net Assessment in ongoing DIW Assessment (95-96).
  - GEN Larry Welch (President) appointed to Security Policy Advisory Board in 1996.
  - Have developed and conducted training and education courses on computer security.
  - Operate supercomputing research center in support of NSA. Have additional high performance computing research underway at LaJolla, CA, and Princeton, NJ.
  - Operate a simulation center. Attempting to define how to simulate the effects of IW.
- Conducted DARPA-sponsored invited workshops on Security in Optical Systems, Survivability, and Security in next-generation Command and Control Systems.
- Completed a Central Research Project on IW to identify and examine concepts and relevant activities associated with DoD initiatives. Paper intended to provide a foundation and starting point from which to address issues of requirements, strategy acquisition and implementation.
- Conducted analysis and review for the Commission on Roles and Missions of the Armed Forces (CORM) on IW concepts and linkages to Command, Control, Communications & Intelligence (C3I) topics and issues.
- Provides analyses for the Joint Staff (JS) of the conduct and lessons learned with respect to IW and Command & Control Warfare (C2W) during the extensive Bosnia air operations campaign from 1992-1995.

This page intentionally left blank.

Executive Branch

Executive Branch

This page intentionally left blank.



National Economic Council
L. Tyson

Director of Science and Technology
T. Kalil

Organization: National Economic Council (NEC)

Senior Information Assurance Official:

Hon. Laura Tyson, Assistant to the President for Economic Security

Information Assurance Points of Contact:

Tom Kalil, Director of Science and Technology, NEC Staff

On-Line Resources:

NEC Homepage: http://www1.whitehouse.gov/WH/EOP/nec/html/main.html

Information Assurance Related Missions and Functions:

The NEC was created by Executive Order on January 25, 1993. Its primary functions are to:

Coordinate the economic policy-making process with respect to domestic and international economic issues.

Coordinate economic policy advice to the President.

Ensure the economic policy decisions and programs are consistent with the President's stated goals and to ensure that those goals are being effectively pursued.

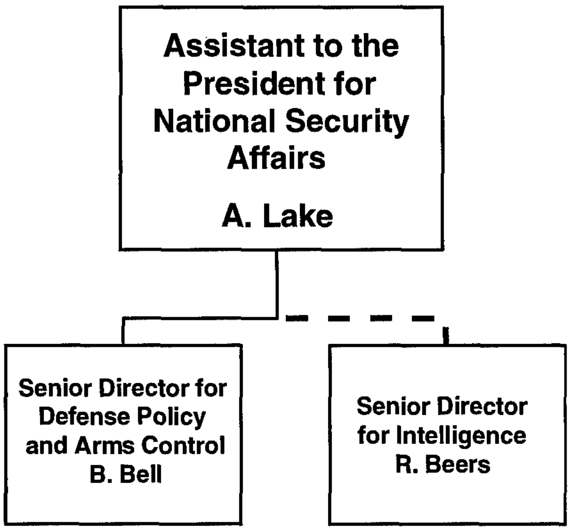
Monitor implementation of the President's economic policy agenda.

Information Assurance Activities, Issues, Best Practices, Lessons Learned:

The NEC and the Office of Science and Technology Policy collaborated on planning for the Information Infrastructure Task Force, which was established by Vice President Gore and is chaired by Hon. Ron Brown, Secretary of Commerce. Mr. Kalil continues to be actively involved in IITF activities.

Mr. Kalil is also involved in cryptology policy issues such export controls and key escrow considerations.

National Security Council Staff



Assistant to the President for National Security Affairs
A. Lake

Senior Director for Defense Policy and Arms Control
B. Bell

Senior Director for Intelligence
R. Beers

Organization: National Security Council (NSC) Staff

Senior Information Assurance Official:

Bob Bell, Senior Director for Defense Policy and Arms Control, NSC

Information Assurance Points of Contact:

CAPT Joe Sestak, Director for Defense Policy, NSC Staff
Randy Beers, Senior Director for Intelligence, NSC Staff
Ed Appel, Director for Counterintelligence, NSC Staff

On-Line Resources:

NCS Homepage: http://www.whitehouse.gov/WH/EOP/html/other/NSC-plain.html

Information Assurance Related Missions and Functions:

Members are the President, the Vice President, the Secretary of State, and the Secretary of Defense. The Director of Central Intelligence and the Chairman of the Joint Chiefs of Staff are statutory advisors for intelligence and military matters, respectively.

The Secretary of the Treasury, the U.S. Trade Representative, the Chief of Staff to the President, and the Assistants to the President for National Security Affairs and Economic Policy are invited to all meetings of the Council.

The Council advises and assists the President in integrating all aspects of national security policy as it affects the United States -- domestic, foreign, military, intelligence, and economic -- in conjunction with the National Economic Council.

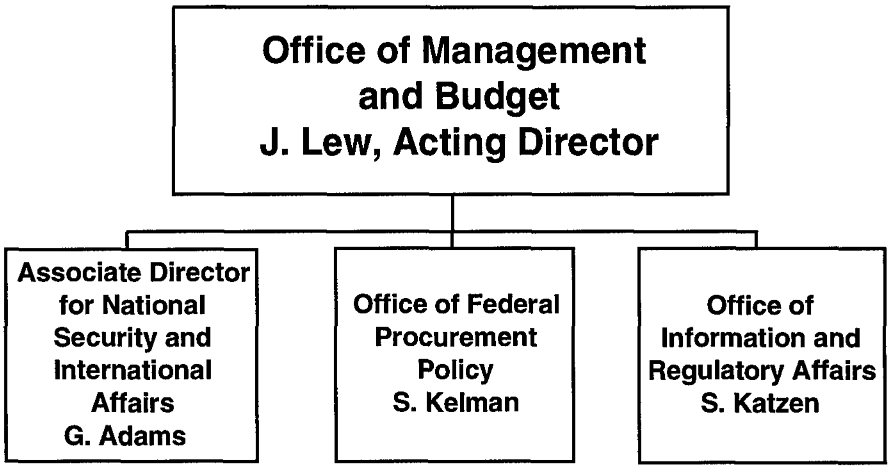
Information Assurance Activities, Issues, Best Practices, Lessons Learned:

- The Defense Policy and Arms Control Office headed by Bob Bell has the lead for information operations and assurance.
- The Intelligence Office headed by Randy Beers handled the Clipper and data encryption issues. Mr. Ed Appel of this office also has oversight over the U.S. Security Policy Board.
- The 1995 national security strategy includes economic security which has implications in terms of roles and responsibilities for infrastructure protection and information assurance. In addition, the 1996 strategy includes the following statement:

> "Finally, the threat of intrusions to our military and commercial information systems poses a significant risk to national security and is being addressed." [A National Security Strategy of Engagement and Enlargement, The White House, February, 1996]

- NSC initiated a review of the policy formulation process associated with information assurance and infrastructure protection. The results of that review will be implemented soon.
- The President's National Security Telecommunications Advisory Committee (NSTAC) asked for a focal point for information assurance in March 1995. The National Security Advisor was named as the focal point and is assisted in this role by the Senior Director for Defense Policy and Arms Control and his staff.

This page intentionally left blank.



Office of Management and Budget
J. Lew, Acting Director

Associate Director for National Security and International Affairs
G. Adams

Office of Federal Procurement Policy
S. Kelman

Office of Information and Regulatory Affairs
S. Katzen

Organization: Office of Management and Budget

Senior Information Assurance Official:

Sally Katzen, Administrator, Office of Information and Regulatory Affairs

Information Assurance Points of Contact:

Bruce McConnell, Chief, Office of Information and Regulatory Affairs
Ed Springer, Office of Information and Regulatory Affairs

On-Line Resources:

OMB Homepage: http://www.whitehouse.gov/WH/EOP/omb

Information Assurance Related Missions and Functions:

The Office of Management and Budget evaluates, formulates, and coordinates management procedures and program objectives within and among Federal departments and agencies. Some of its primary responsibilities are to assist the President in developing and maintaining effective government, assist in developing efficient coordinating mechanisms to expand interagency cooperation, assist the President in preparing the budget, assist in developing regulatory reform proposals and programs for paperwork reduction, especially reporting burdens of the public, to plan and develop information systems that provide the President with program performance data, and to improve the economy, efficiency, and effectiveness of the procurement process.

The Office of Management and Budget establishes Federal policy for the security of Federal automated information systems in OMB Circular No. A-130. Appendix III of the Circular requires Federal agencies to establish computer security programs and sets minimum requirements for such programs. The circular applies to the activities of all agencies of the Executive Branch. A revised Circular No. A-130 was distributed in February 1996 that included significant changes to Appendix III. National security information and national security emergency preparedness activities are subject to additional regulations under appropriate directives and executive orders.

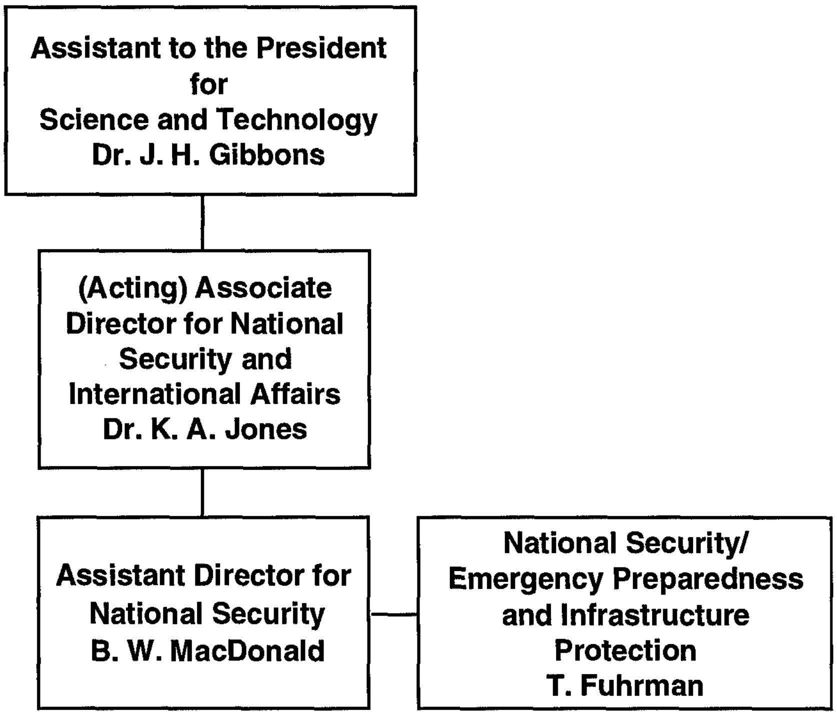
OMB Circular No. A-130, Management of Federal Information Resources, is issued pursuant to OMB's authorities under the Paperwork Reduction Act, (44 U.S.C., Chapter 35), the Privacy Act (5 U.S.C. 552A), the Chief Financial Officers Act (31 U.S.C. 3512 et seq), the Federal Property and Administrative Services Act (40 U.S.C. 759 and 487), the Computer Security Act (40 U.S.C. 759 note), the Budget and Accounting Act (31 U.S.C. Chapter 11), Executive Order 12046 and Executive Order 12472

Information Assurance Activities, Issues, Best Practices, Lessons Learned:

- The OMB mission for infrastructure assurance is to ensure that all stakeholders are involved in the dialogue from the beginning. This is difficult because infrastructure assurance cuts across so many sectors and interests, but public participation is essential if infrastructure protection efforts are to succeed.
- Government doesn't own the infrastructure, therefore protection often requires regulation and participation from the public sector.
- A-130 Appendix III (security appendix) has been updated.
  - There is no longer a requirement for an agency information security official.
  - There is no longer a requirement to certify the security controls in sensitive applications.
  - There is no longer a requirement for an agency-level information security program; training is now required to be specific for systems.
  - The requirement for the performance of formal risk analysis, as an element of an agency information security has been deleted. The requirement is for management of risk rather than measurement of risk.
  - There is a new requirement for the incident response capabilities at the system level.
  - A new requirement for the inclusion of a summary of agency security plans in the information resources management plan required by Paperwork Reduction Act.
- The goal of the A-130 revision was to ensure that security is built into management control. Security is a personnel and management issue and A-130 imbeds security as a responsibility for both employees and managers. It recognizes the human aspect of security.
- OMB is a member of the Critical Infrastructure Working Group. The group has been established administratively, but funding has impacted performance.
- OMB now co-chairs the Inter-Agency Working Group on Cryptography.
- There is increased citizen awareness of information technology and of government information technology activity.
- Policy areas of concern include: intellectual property rights, software protection privacy, security (NII Security Plan due out shortly).
- National Performance Review implementation underway through Government Information Technology Services (GITS).

This page intentionally left blank.

Office of Science and Technology Policy



Assistant to the President for Science and Technology Dr. J. H. Gibbons

(Acting) Associate Director for National Security and International Affairs Dr. K. A. Jones

Assistant Director for National Security B. W. MacDonald

National Security/ Emergency Preparedness and Infrastructure Protection T. Fuhrman

Organization: Office of Science and Technology Policy (OSTP)

Senior Information Assurance Officials:

Dr. Kerri-Ann Jones, Acting Associate Director for National Security and International Affairs
Bruce MacDonald, Assistant Director for National Security

Information Assurance Points of Contact:

Tom Fuhrman, National Security and International Affairs Division
Dr. Mike Nelson, Special Assistant for Information Technology

On-Line Resources:

OSTP Homepage: http://www.whitehouse.gov/OSTP.html

Information Assurance Related Missions and Functions:

The Office of Science and Technology Policy (OSTP) was established by the National Science and Technology Policy, Organization, and Priorities Act of 1976 (Public Law 94-282). OSTP's responsibilities are to:

- Advise the President in policy formulation and budget development on all questions in which science and technology (S&T) are important elements.
- Lead an interagency effort to develop and implement S&T policies and budgets that are coordinated across Federal agencies.
- Articulate the President's S&T policies and programs to the Congress, and address and defend the need for appropriate resources.
- Foster strong partnerships among Federal, State, and local governments, and the scientific communities in industry and academe.
- Further international cooperation in science and technology activities.

OSTP's Director also serves as the Assistant to the President for Science and Technology. In this capacity, he manages the National Science and Technology Council (NSTC) and the President's Committee of Advisors on Science and Technology (PCAST).

The NSTC is a Cabinet council, chaired by the President, that acts as a "virtual" agency for science and technology to coordinate the diverse parts of the Federal R&D enterprise. PCAST is a committee of distinguished individuals appointed by the President to provide private sector advice in the S&T policy making process.

OSTP is led by a Director and four Associate Directors, all of whom are Presidentially-appointed and Senate-confirmed. OSTP is organized into four divisions:

Science Division

The Associate Director for Science leads the White House effort to ensure that: 1) the United States continues to maintain global leadership in science, mathematics, and engineering research; and (2) science continues to provide support for the successful resolution of some of the most important problems in the areas of health, agriculture, the economy, energy, social well-being, education, and national security. The Division focuses on maintaining a broad Federal research program that advances the frontiers of knowledge, is based on excellence, strongly coupled to education, and supportive of critical national goals.

Technology Division

The Associate Director for Technology leads the White House effort to develop and implement federal policies for harnessing technology to serve national goals such as global economic competitiveness, environmental quality, and national security. The Division's priorities include: redirecting the U.S. space and aeronautics program, including the space station; sustaining U.S. leadership in defense technology while increasing the focus on dual use and civilian technologies; advancing technologies for education and training for all learning environments; and facilitating development and adoption of advanced manufacturing technologies and advanced computing and communications technologies.

Environment Division

The Associate Director for Environment leads the White House efforts to: 1) ensure a sound scientific and technical underpinning for environmental policies, and 2) develop an interagency R&D strategy for environment and natural resource issues.

National Security and International Affairs Division

The Associate Director for National Security and International Affairs leads the White House effort to use science and technology in the service of our national security, and to shape and coordinate international cooperation in S&T. The national security agenda includes: defense technology investments in an era of downsizing; technical aspects of arms control and nonproliferation policy; technology transfer and related export control policies; and intelligence technology. The international agenda includes: using U.S. leadership in S&T to support U.S. foreign policy objectives; strengthening American S&T in the context of an increasingly interdependent world; using international cooperation in S&T to support economic goals; and enhancing international cooperation in large-scale science programs. The Associate Director for National Security and International Affairs also serves as the Senior Director for Science and Technology of the National Security Council staff.

OSTP also plays a key role in formulating a national strategy to advance the development and evolution of the National Information Infrastructure.

In addition, the National Security and International Affairs Division is responsible for all of OSTP's activities in the areas of national security/emergency preparedness, emergency telecommunications, the National Communications System, the National Security Telecommunications Advisory Committee, Continuity of Government programs and infrastructure protection programs, and works closely with the Technology Division on national information infrastructure issues.

OSTP has official responsibilities in protecting the domestic infrastructure deriving both from statute and executive order. As a result OSTP is in a unique position to bridge the cultural divides existing between the military and non-military sectors within the government, between the technical and the policy-making communities, and between the Federal government and state and local governments. The following activities are representative of the major responsibilities of OSTP:

> Statutory Role of OSTP. By statute, OSTP serves as a "source of scientific and technological analysis and judgment for the President with respect to major policies, plans, and programs of the Federal government." The statute further states that the Director of OSTP shall "seek to define coherent approaches for applying science and technology to critical and emerging national and international problems and for promoting coordination of the scientific and technological responsibilities and programs of the Federal departments and agencies in the resolution of such problems." (42 USC 6614)
>
> Emergency Telecommunications Authorities. By Executive Order, the OSTP Director is assigned responsibility for directing the exercise of the President's wartime authorities over domestic telecommunications which derive from the Communications Act of 1934. In emergencies or crises in which the exercise of the President's war power functions is not required or permitted by law, the OSTP Director is charged with the responsibility to advise and assist the President and Federal departments and agencies with the provision, management, or allocation of telecommunications resources. The National Communications System (NSC), a formal interagency organization, assists the President, the OSTP Director, the National Security Advisor, and the Director of OMB in the exercise of national security and emergency preparedness telecommunications functions. (47 CFR 201,202)
>
> Responsibilities under the Federal Response Plan. The Robert T. Stafford Disaster Relief and Emergency Assistance Act provides the authority to the Federal government to respond to disasters and emergencies in order to provide assistance to save lives and protect public health, safety, and property. The Federal Response Plan is designed to address the consequences of any disaster or emergency situation in which there is a need for Federal response assistance under the authorities of the Stafford Act. OSTP is responsible for the communications portion of the Federal Response Plan, which addresses Federal telecommunications support to federal, state, and local response efforts following a Presidentially declared emergency, major disaster, extraordinary situation, or other emergency. (42 USC 5121)

National Security Telecommunications Advisory Committee (NSTAC). Executive Order 12382 established the NSTAC, a Presidentially-appointed private sector advisory group, to advise the President on telecommunications matters related to national security/emergency preparedness. OMB, OSTP, and the National Security Council are the NSTAC focal points within the Executive Office of the President, and participate with the Industry Executive Subcommittee in defining the NSTAC agenda.

International Science and Technology Cooperation. OSTP fosters inter-governmental cooperation in science and technology, including coordination of international information network development.

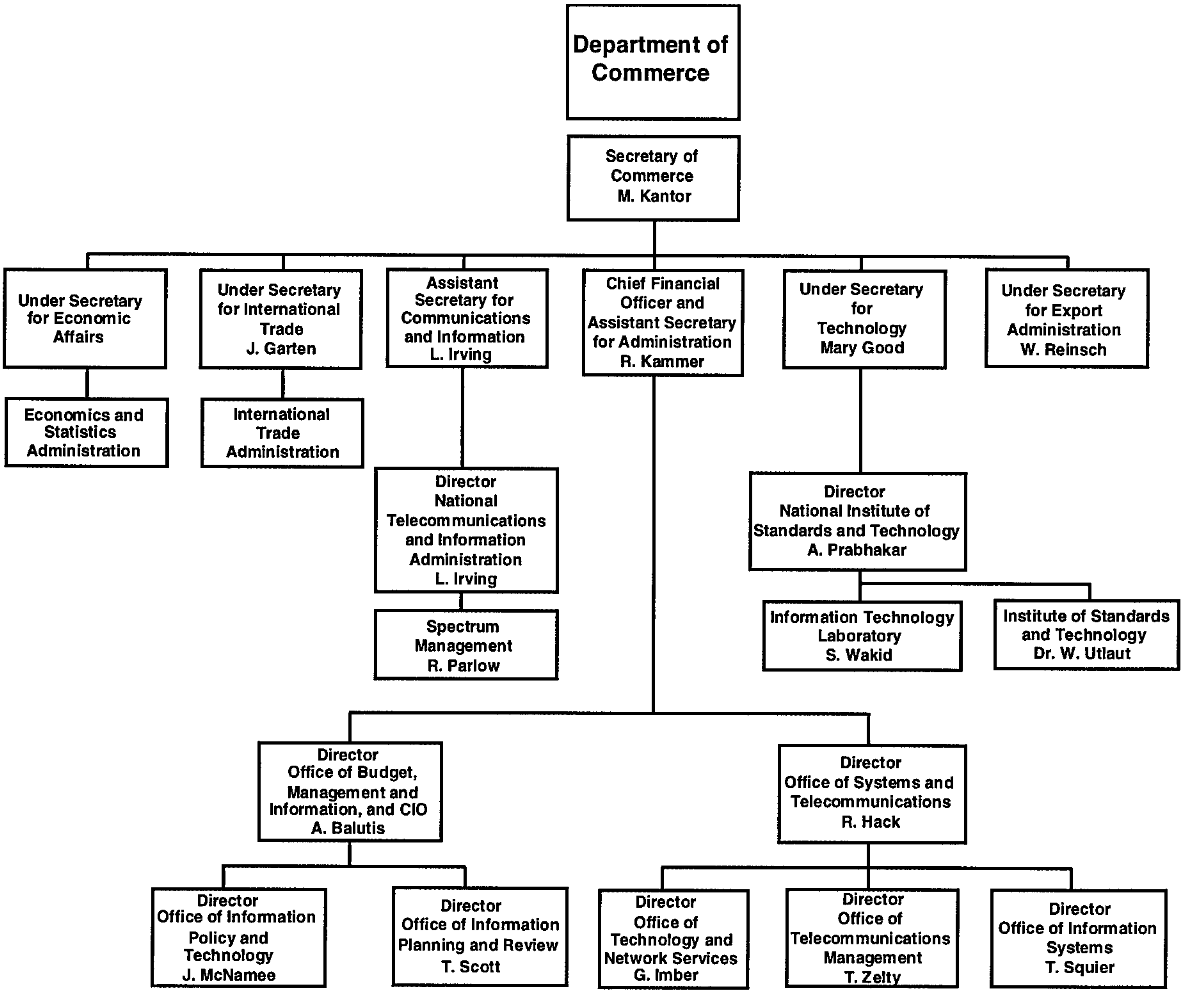
Linkage with the States. The State-Federal Technology Partnership Task Force, which was established by a Presidential directive and is supported by OSTP, seeks to engage federal and state governments in a formal process to represent States at the highest national policy level on science and technology issues. In addition, OSTP has important links with State and regional emergency preparedness activities related to the information infrastructure through association with the National Communications System and the Federal Emergency Management Agency.

Technical Expertise. The technical and policy expertise resident at OSTP includes information networks, computers, and communications systems, and emergency telecommunications services. OSTP also maintains professional relationships with the broader national scientific and technical community.

Information Assurance Activities, Issues, Best Practices, Lessons Learned:

- OSTP is actively involved in all National Information Infrastructure Task Force activities to include fostering the development of the Global Information Infrastructure.
- A white paper entitled "Towards an Analytical Framework for Infrastructure Protection Policy" describes an analytical approach to assessing the technical aspects of network-related infrastructure vulnerabilities.

This page intentionally left blank.


Department of Commerce
Secretary of Commerce M. Kantor
Under Secretary for Economic Affairs
Economics and Statistics Administration
Under Secretary for International Trade J. Garten
International Trade Administration
Assistant Secretary for Communications and Information L. Irving
Director National Telecommunications and Information Administration L. Irving
Spectrum Management R. Parlow
Chief Financial Officer and Assistant Secretary for Administration R. Kammer
Under Secretary for Technology Mary Good
Director National Institute of Standards and Technology A. Prabhakar
Information Technology Laboratory S. Wakid
Institute of Standards and Technology Dr. W. Utlaut
Under Secretary for Export Administration W. Reinsch
Director Office of Budget, Management and Information, and CIO A. Balutis
Director Office of Information Policy and Technology J. McNamee
Director Office of Information Planning and Review T. Scott
Director Office of Systems and Telecommunications R. Hack
Director Office of Technology and Network Services G. Imber
Director Office of Telecommunications Management T. Zelty
Director Office of Information Systems T. Squier

Organization: Department of Commerce (DoC)

Senior Information Assurance Official:

Raymond Kammer, Chief Financial Officer and Assistant Secretary for Administration

Information Assurance Points of Contact:

Alan Balutis, Director, Office of Budget, Management, and Information
R. Hack, Director, Office of Systems and Telecommunications
G. Imber, Director Office of Technical Support and Network Services
Tom Scott, Director, Office of Information Planning and Review
J. Squier, Director, Office of Information Systems
Tom Zetty, Director, Office of Telecommunications Management

On-Line Resources:

DoC Homepage: http://www.doc.gov

Information Assurance Related Missions and Functions:

The Department of Commerce encourages, serves, and promotes the Nation's international trade, economic growth, and technological advancement. It offers assistance and information to increase America's competitiveness in the world economy; administers programs to prevent unfair foreign trade competition; provides social and economic statistics and analyses for business and government planners; provides research and support for the increased use of scientific, engineering, and technological development; grants patents and registers trademarks; develops policies and conducts research on telecommunications; and provides assistance to promote domestic economic development. It carries out these responsibilities in the Office of the Secretary and its operating units, a selected number of which are described below.

The Bureau of Export Administration is responsible for directing the Nation's export control policy in accordance with the Export Administration Act and the Export Administration Regulations. The Bureau maintains a Commerce Control List of sensitive or dual-use items including software and scientific and technical data which is maintained for national security purposes, to prevent the items from reaching proscribed countries, and for various foreign policy objectives. It exercises control by processing export license applications, conducting foreign availability studies to determine when products should be decontrolled, and enforcing U.S. export control laws.

The International Trade Administration is responsible for promoting world trade and for strengthening the international trade and investment position of the United States. The Bureau of Export Administration and the International Trade Administration were created by law to be separate organizational entities within the Department. In addition to directing the

International Trade Administration, the Under Secretary for International Trade also supervises the U.S. and Foreign Commercial Service. The USFCS develops, produces, markets, and manages an effective line of high-quality products and services geared to the marketing information needs of the U.S. exporting and international business community and manages the delivery of Administration programs through 47 domestic offices and U.S. export assistance centers located in the United States and 132 posts located in 68 countries throughout the world.

The National Oceanic and Atmospheric Administration mission is to explore, map, and chart the global ocean, to describe, monitor, and predict conditions in the atmosphere, ocean, Sun, and space environment, to issue warnings against impending destructive natural events, and to disseminate long-term environmental information. Its principal field organizations include the National Weather Service, the National Marine Fisheries Service, the National Environmental Satellite, Data, and Information Service, the National Ocean Service, and the Office of Oceanic and Atmospheric Research.

The National Telecommunications and Information Administration responsibilities are described in a separate organizational summary.

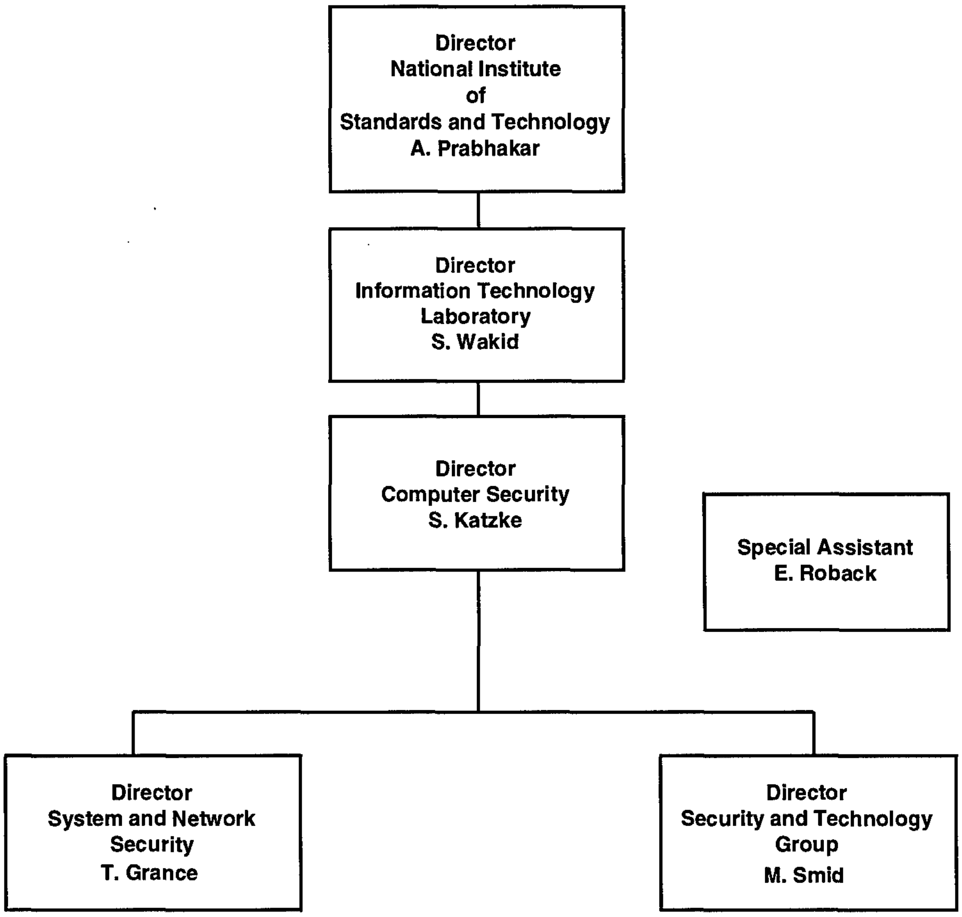
The Technology Administration is responsible for working with U.S. industry in addressing competitiveness issues. It discharges this role through the Office of Technology Policy by advocating coherent policies for maximizing the impact of technology on economic growth, through the National Institute for Standards and Technology (NIST) by carrying out technology programs with U.S. industry, and through the National Technical Information Service by disseminating technology information. Specific National Institute for Standards and Technology responsibilities are described in a separate organizational summary.

The Under Secretary of Commerce advises the Secretary and other Government officials on matters relating to economic developments and forecasts and on the development of macroeconomic and microeconomic policy. The Under Secretary, as the Administrator of the Economics and Statistics Administration, exercises general supervision over the Bureau of the Census and the Bureau of Economic Analysis. The Bureau of the Census collects, tabulates and published a wide variety of statistical data about the people ant the economy of the Nation. The goal of the Bureau of Economic Analysis is to provide a clear picture of the U.S. economy through the preparation, development, and interpretation of the national income and product accounts, summarized by numerous indicators such as the gross domestic product, input-output accounts, etc.

Information Assurance Activities, Issues, Best Practices, Lessons Learned:

- Standards developed by NIST are released by the Department of Commerce. The Department of Commerce and GSA publish Federal Information Processing Standards.
- Like many other Departments, Commerce is becoming smaller. Ten thousand positions have been eliminated in the last four years; 500 within the last 60 days. The Commerce budget will probably decrease ten to twenty percent in the next fiscal year.

This page intentionally left blank.


Director
National Institute
of
Standards and Technology
A. Prabhakar
Director
Information Technology
Laboratory
S. Wakid
Director
Computer Security
S. Katzke
Special Assistant
E. Roback
Director
System and Network
Security
T. Grance
Director
Security and Technology
Group
M. Smid

Organization: National Institute of Standards and Technology (NIST)

Senior Information Assurance Official:

Shukri Wakid, Director, Information Technology Laboratory

Information Assurance Points of Contact:

Stuart Katzke, Chief, Computer Security Division
Edward Roback, Computer Specialist, Computer Security Division
Tim Grance, Director, Systems and Network Security
M. Smid, Director, Security Technology Group

On-Line Resources:

NIST Homepage: http://www.nist.gov
NIST Security Activities: http://csrc.ncsl.nist.gov/

Information Assurance Related Missions and Functions:

NIST's primary mission is to promote U.S. economic growth by working with industry to develop and apply technology, measurements, and standards. It does this by assisting industry to develop technology to improve product quality, to modernize the manufacturing process, to ensure product reliability, and to facilitate rapid commercialization of products based on new scientific discoveries.

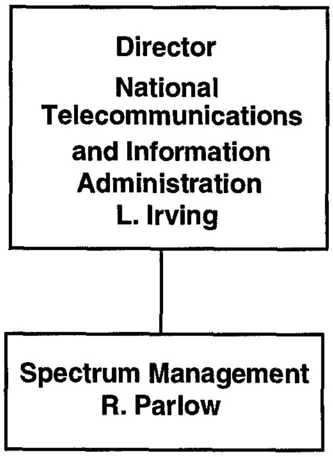
By the Information Technology Management Reform Act of 1996 and the Computer Security Act of 1987, NIST was assigned responsibilities to develop government-wide computer system security standards and guidelines and security training programs for the protection of sensitive unclassified information maintained in Federal government computer systems. NIST also administers the Computer System Security and Privacy Advisory Board to advise the Secretary of Commerce and the Director of NIST. The Board also identifies emerging computer security issues and informs the Director, Office of Management and Budget, the Director, National Security Agency, the House Committee on Government Operations, and the Senate Committee on Governmental Affairs of security issues. These responsibilities are carried out by the Information Technology Laboratory (ITL).

Information Assurance Activities, Issues, Best Practices, Lessons Learned:

- NIST has approximately 35 people and a base budget of $3.0 million augmented by approximately $3.5 million in other agency funding to fulfill the above responsibilities.
- Significant accomplishments include Data Encryption Standard, Digital Signature Standard, Federal Information Processing Standard (FIPS) 186.

- Debate leading to Computer Security Act of 1987 provides very useful historical perspective. Suggested review of House Government Operations and House Science and Technology Committee reports regarding the legislation.
- Must identify some incremental approach which has cost realism. Policy issues for the private sector must be translated into cost.
- NIST administers the Computer System Security and Privacy Advisory Board which was created by Computer Security Act of 1987. Board consists of volunteers. In general, board is not resourced to properly do its job. Its impact to date has been minimal. The Board's membership and activities are outlined in a separate organizational summary.
- Many of the recommendations made in the NRC report "Computers at Risk" are still valid. Example is recommendation to establish Information Security Foundation.
- The Interagency Working Group on Cryptographic Policy is chaired by Bruce McConnell of the Office of Management and Budget and Ed Appel of the National Security Council Staff. It includes membership from NIST, NSA, *DoC*, DoJ, FBI, DoS, CIA, Treasury, and others.
- Government Information Technology Service group IT-10 recommended that NIST develop Generally-Accepted Systems Security Practices (GSSP). Stu Katzke is involved in the effort. Expect to publish by mid-1996.
- Information Systems Security Association is also involved in publication of their own GSSP.
- NIST co-chairs the Federal Computer Security Program Manager's Forum which is described in a separate organizational summary.
- NIST is developing an ITL testing center with special emphasis on security.
- NIST is one of the co-founders of the Forum of Incident Response and Security Teams and until recently provide secretariat services for FIRST.
- NIST acts as resource clearing house for computer security matters and has recently published a computer security handbook
- Pending legal review and approval, NIST will establish a computer emergency response capability to aid Federal departments and agencies in satisfying the recent mandate (Revised Appendix III to OMB Circular A-130) for a such a capability. This capability will be provided on a cost-reimbursable basis using the Department of Energy's Computer Incident Advisory Capability and the Software Engineering Institute's Computer Emergency Response Team.
- In June 1996, NIST co-sponsored a conference on vulnerabilities with the intent of developing a modest pilot mechanism for sharing vulnerability information. Other sponsors included DARPA, NCS, and COAST.

This page intentionally left blank.


Director
National
Telecommunications
and Information
Administration
L. Irving
Spectrum Management
R. Parlow

Organization: National Telecommunications Information Administration (NTIA)

Senior Information Assurance Official:

Larry Irving, Administrator

Information Assurance Points of Contact:

Dick Parlow, Chief, Office of Spectrum Management
Bill Gamble, Office of Spectrum Management

On-Line Resources:

NTIA Homepage: http://www.ntia.doc.gov

Information Assurance Related Missions and Functions:

The National Telecommunications and Information Administration responsibilities are to serve as the principal executive branch advisor to the President on telecommunications and information policy, to develop and present U.S. plans and policies at international communications conferences and related meetings, to coordinate U.S. Government positions on communications with the Federal Communications Commission, the U.S. Department of State, and other Federal agencies, to prescribe policies for and managing Federal use of the radio frequency spectrum, to serve as the principal Federal telecommunications research and engineering laboratory through the Institute for Telecommunications Sciences, to provide grants through the Telecommunications and Information Infrastructure Assistance Program (TIIAP) for planning and demonstration projects to promote the development and widespread availability of advanced telecommunications technologies, to provide grants through the Public Telecommunications Facilities Program to extend delivery of public telecommunications services to U.S. citizens and to strengthen the capabilities of existing public broadcasting stations to provide telecommunications services.

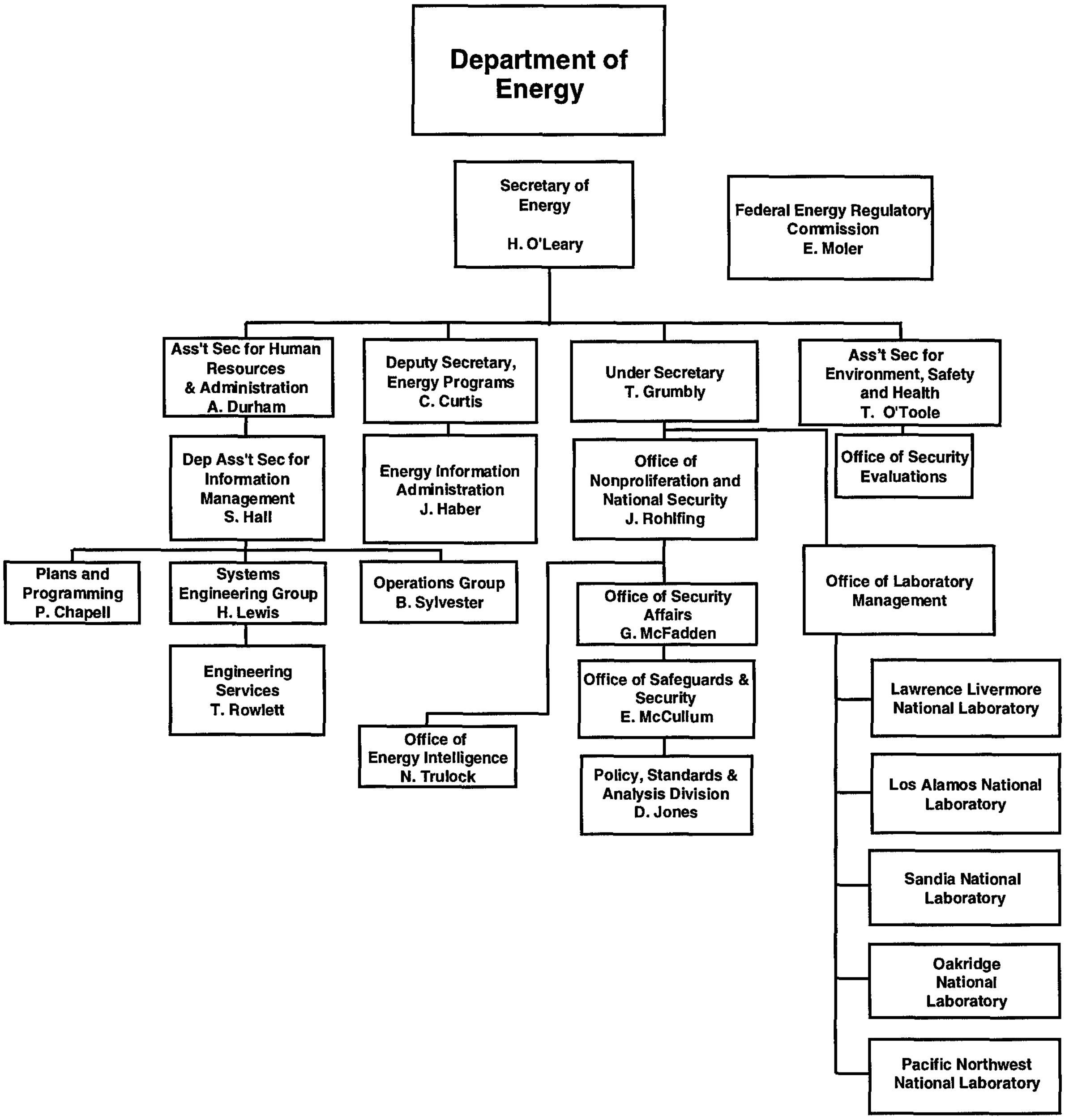
Information Assurance Activities, Issues, Best Practices, Lessons Learned:

- NTIA has been a participant in most Information Infrastructure Task Force committees and working groups. NTIA is actively involved in all wireless activities related to IITF.
- NTIA also participates in bilateral activities related to deregulation, opening markets, etc. Other participants include Office of U.S. Trade Representative, International Trade Administration, and DoS.
- The Institute of Telecommunications Sciences at Boulder, CO, does telecommunications research (e.g., propagation characteristics). ITS also participates in standards development for wireline environment.
- NTIA administers the Telecommunications and Information Infrastructure Assistance Program, a grant program appropriated $21.5M for FY96 by enactment of Public Law 104-134 on April 26, 1996. In all, 809 applications requesting a total amount of $260M

were received from 50 states, the District of Columbia, and the Commonwealth of Puerto Rico.

- NTIA also administers the Public Telecommunications Facilities Program, a grant program appropriated $15.5M for FY96.
- Further information can be obtained from the Director, Public Broadcasting Division, Dennis Connors, Telephone: 202-482-1835, Fax: 202482-2156, E-mail: ptfp@ntia.doc.gov, and from the Acting Director, Telecommunications and Information Infrastructure Assistance Program, Stephen J. Downs, Telephone: 202-482-2048, Fax: 202-501-5136, E-mail: tiiap@ntia.doc.gov.

This page intentionally left blank.


Department of Energy
Secretary of Energy
H. O'Leary
Federal Energy Regulatory Commission
E. Moler
Ass't Sec for Human Resources & Administration
A. Durham
Deputy Secretary, Energy Programs
C. Curtis
Under Secretary
T. Grumbly
Ass't Sec for Environment, Safety and Health
T. O'Toole
Dep Ass't Sec for Information Management
S. Hall
Energy Information Administration
J. Haber
Office of Nonproliferation and National Security
J. Rohlfing
Office of Security Evaluations
Plans and Programming
P. Chapell
Systems Engineering Group
H. Lewis
Operations Group
B. Sylvester
Office of Security Affairs
G. McFadden
Office of Laboratory Management
Engineering Services
T. Rowlett
Office of Safeguards & Security
E. McCullum
Office of Energy Intelligence
N. Trulock
Policy, Standards & Analysis Division
D. Jones
Lawrence Livermore National Laboratory
Los Alamos National Laboratory
Sandia National Laboratory
Oakridge National Laboratory
Pacific Northwest National Laboratory

Organization: Department of Energy (DoE)

Senior Information Assurance Official:

Gen. George L. McFadden, Jr., Director, Office of Security Affairs
Spain W. Hall, Jr., Deputy Assistant Secretary for Information Management

Information Assurance Points of Contact:

Larry Wilcher, Program Manager, Information Assurance Program
Tom Rowlett, Director, Engineering Services, Systems Engineering Group, Information Resources Management
Brent Frampton, Computer Security Specialist, Energy Information Administration
Mary Beth Davis, Deputy Director, Office of Energy Intelligence

On-Line Resources:

DoE Homepage: http://www.ntia.doc.gov/

Information Assurance Related Missions and Functions:

The Department of Energy provides the framework for a comprehensive and balanced national energy plan throughout the coordination and administration of the energy functions of the Federal government. The Department is also responsible for energy regulatory programs and a central energy data collection and analysis programs.

The Office of Non Proliferation and National Security safeguards and secures classified information and protects Departmental and Department of Energy contractor facilities, National Laboratories and installations, manages the Department's Emergency Management System, which responds to and mitigates the consequences resulting from operational, energy, and continuity of Government emergencies.

The Office of Energy Intelligence detects and defeats foreign intelligence services bent on acquiring sensitive information on the Department's programs, facilities, technology, and personnel.

The Office of Information Resources Management is responsible for development and implementation of policy regarding the protection of sensitive but unclassified information.

The Office of the Assistant Secretary for Environment, Safety, and Health is responsible for independent oversight of nuclear/non-nuclear safety and security laws, regulations, and policies.

The Energy Information Administration is responsible of the timely and accurate collection, processing, and publication of data in the areas of energy resource reserves, energy production, demand, consumption, distribution and technology.

The Federal Energy Regulatory Commission is responsible for setting rates and charges for the transportation and sale of natural gas and for the transmission and sale of electricity and the licensing of hydroelectric power projects.

The Office of Laboratory Management is responsible for institutional policy and oversight functions related to utilization of the Department of Energy's multiprogram laboratories to assure optimum utilization of the Department's laboratory complex for meeting national research and technology development objectives. Organizational summaries for the Lawrence Livermore National Laboratory, the Los Alamos National Laboratory, Sandia National Laboratories, Oak Ridge National Laboratory, and Pacific Northwest National Laboratory follow.

Information Assurance Activities, Issues, Best Practices, Lessons Learned: (Rewrite)

- Information security responsibilities split in DoE. Office of IRM responsible for unclassified information (to include connections to Internet). Office of Nonproliferation and National Security responsible for classified information. Office of Energy Intelligence.
- Office of IRM currently working on a DoE policy for sensitive unclassified information with primary emphasis on encypherment.
- The Assistant Secretary for Environment, Safety, and Health operates an Office of Security Evaluations.
- DOE's ESNet is primary backbone of Internet.
- Office of IRM's Engineering Services and the Office of Safeguards and Security sponsor the Computer Incident Advisory Capability (CIAC) operated by the Lawrence Livermore National Laboratory. CIAC also provides information security assistance visits as requested.
- Must emphasize responsibilities of information owners and hold them accountable.
- Moving away from specific policy directives to guidance.
- DoE owns National Laboratory facilities and products of research. Laboratories are operated by independent entities, such as the University of California.
- Current DoE information assurance issues:
  - Finding a cohesive and structured approach to a graded system of information protection from unclassified up through the highest levels of classified.
  - DoE Information Assurance Infrastructure.
  - Efforts to identify DoE key assets.
  - There is a lack of funding for security initiatives.

Organization: Lawrence Livermore National Laboratory (LLNL)

Senior Information Assurance Official:

David M. Cooper, Associate Director for Computation

Information Assurance Points of Contact:

Doug L. Mansur, Head, Computer Security Technology Center

On-Line Resources:

LLNL Homepage: http://www.llnl.gov
Computer Incident Advisory Capability: http://ciac.llnl.gov/ciac/notes/

Information Assurance Related Missions and Functions:

The Computer Security Technology Center (CSTC) is an element of the Computation Organization at the LLNL; it serves the needs of clients in the U.S. Department of Energy (DoE) and other federal agencies. The CSTC delivers solutions to today's information technology security challenges through integration of operations; incident response, product development, and consulting services.

Computer Incident Advisory Capability (CIAC) is an element of the CSTC and is also located at LLNL. CIAC provides computer security free of charge to employees and contractors of the DoE; these services include: incident handling, computer security information, on-site workshops, and computer security consulting. CIAC provides operational incident response and serves as the single point of contact for all DoE incident handling. This team gathers fast-breaking vulnerability and threat information and disseminates it throughout the DoE community. CIAC is also a founding member of Forum of Incident Response and Security Teams (FIRST).

Information Assurance Activities, Issues, Best Practices, Lessons Learned:

- The Lawrence Livermore National Laboratory is engaged in a joint effort with the Los Alamos National Laboratory and the Sandia National Laboratories to develop a real-time intrusion detection and response system that can supplement or complement an information assurance program for protecting the Department's information resources.
- Other Information Assurance activities emphasize network security topics, with particular specialization in the areas of network security alarms, vulnerability analyses and profiles, network intrusion detection, security profiles, firewall architecture, education, and tools for security management

Organization: Los Alamos National Laboratory (LANL)

Senior Information Assurance Official:

Debra Rutherford, Program Manager, Safeguards & Security

Information Assurance Points of Contact:

William J. Hunteman, Project Leader, Information Assurance

On-Line Resources:

LANL Homepage: http://www.lanl.gov:8010/

Information Assurance Related Missions and Functions:

The computer networks of the LANL are divided into two parts. One part contains the nuclear weapons information and has no connection to the outside world. It cannot be accessed by anyone from outside the laboratory.

The Computer Research and Applications Group builds fraud detection software for many special purpose projects. Most of the group's research tends to be with on-line training and operating modes, adaptive systems, and neural net type systems.

The Network Anomaly Detection Intrusion Reporter (NADIR) system has been running on the laboratory's network since 1989. The goals of this system are detection, deterrence, and accountability. It is an expert system-an automated audit system. The network, all the nodes attached to it, and all the computers have always had the requirements for forming logs and reporting. NADIR has now taken over the task of looking through these logs and detecting anomalous behavior.

Information Assurance Activities, Issues, Best Practices, Lessons Learned:

- The Los Alamos National Laboratory is engaged in a joint effort with the Lawrence Livermore National Laboratory and the Sandia National Laboratory to develop a real-time intrusion detection and response system that can supplement or complement an information assurance program for protecting the Department's information resources.
- The Los Alamos National Laboratory is heavily engaged in short-term on-site support for Departmental entities. This support emphasizes response to unique or critical requirements, or those which involve specialized expertise. Support may include conducting assessments or providing security advice and assistance in all phases of system design, development, and implementation.

Organization: Oak Ridge National Laboratory (ORNL)

Senior Information Assurance Official:

George A. Dailey, Director, Data Systems Research and Development Program

Information Assurance Points of Contact:

Sharon Jacobsen, Manager, Communications and Security Department

On-Line Resources:

ORNL Homepage: http://www.ORNL.gov

Information Assurance Related Missions and Functions:

The Data Systems Research and Development (DSRD) Department of Energy (DoE) Center for Information Security Technology (CIST) was established in 1986 as a joint sponsorship by the Department of Energy and the Department of State. CIST provides support at the national level for a variety of federal agencies, as well as for the Department of Energy and Lockheed Martin Energy Systems. The CIST mission is to provide research, development, demonstration, and application testing and evaluation of information security technologies focusing on the assessment of technologies for use in the classified and unclassified sensitive sectors.

A staff of information security professionals with state-of-the-art technology resources focuses on the protection of classified and unclassified systems for processing information up to and including Top Secret. The experience gained from information management applications that include major accounting and financial transactions, command and control, law enforcement, and many other diverse areas of government concern is available to all CIST activities.

Information Assurance Activities, Issues, Best Practices, Lessons Learned:

- The Oak Ridge National Laboratories are responsible for developing and delivering training and education in all areas of DOE Automated Information System Security. Subject matter ranges from regulatory to technical, and is targeted at all personnel involved with information systems security including managers, information system security professionals, and system users. Additional activity is devoted to secure distributed databases, developing a Multilevel Secure (MLS) Local Area Network, and developing an MLS document storage and retrieval system.

Organization: Pacific Northwest National Laboratory (PNNL)

Senior Information Assurance Official:

Thomas R. Fox, Associate Laboratory Director, National Security Division

Information Assurance Points of Contact:

D. R. Miles, Staff Scientist, DOE Information Security Resource Center

On-Line Resources:

PNNL Homepage: http://www.pnl.gov

Information Assurance Related Missions and Functions:

The Information Security Resource Center (ISRC) collects, analyzes, and disseminates information germane to the Department's Information Assurance activities. Sources include public networks, telecommunication industry sources, Government Agencies, and the Department Contractor Complex. Open source information regarding subjects relating to the protection and integrity of the Department's sensitive information is also collected and analyzed. Information acquisition and analysis is also intended to support policy development.

Information of interest includes that related to protecting information, information systems, and key information resource assets (e.g., telephone systems, power systems, networks). Emphasis is placed on acquisition of information which facilitates development of layered, risk-management-based defenses to guard against attacks on information resources and information assets. Other functions include coordinating protection of information and key information resource assets and ensuring coordination of programmatic and Information Assurance managers.

Information Assurance Activities, Best Practices, Lessons Learned:

- The Pacific Northwest National Laboratories are developing and implementing a database for threat information, and designing and evaluating advanced concepts for data retrieval and analysis. Current initiatives include development of visualization methodologies, technologies, and tools for application to databases which are characterized by having large quantities of data in which the information content is obscured or not readily identifiable by traditional means.

Organization: Sandia National Laboratory (SNL)

Senior Information Assurance Official:

Samuel G. Varnado, Director, Information Systems Engineering Center

Information Assurance Points of Contact:

Patricia C. Sprauer, Program Manager, Information Assurance Research and Development

On-Line Resources:

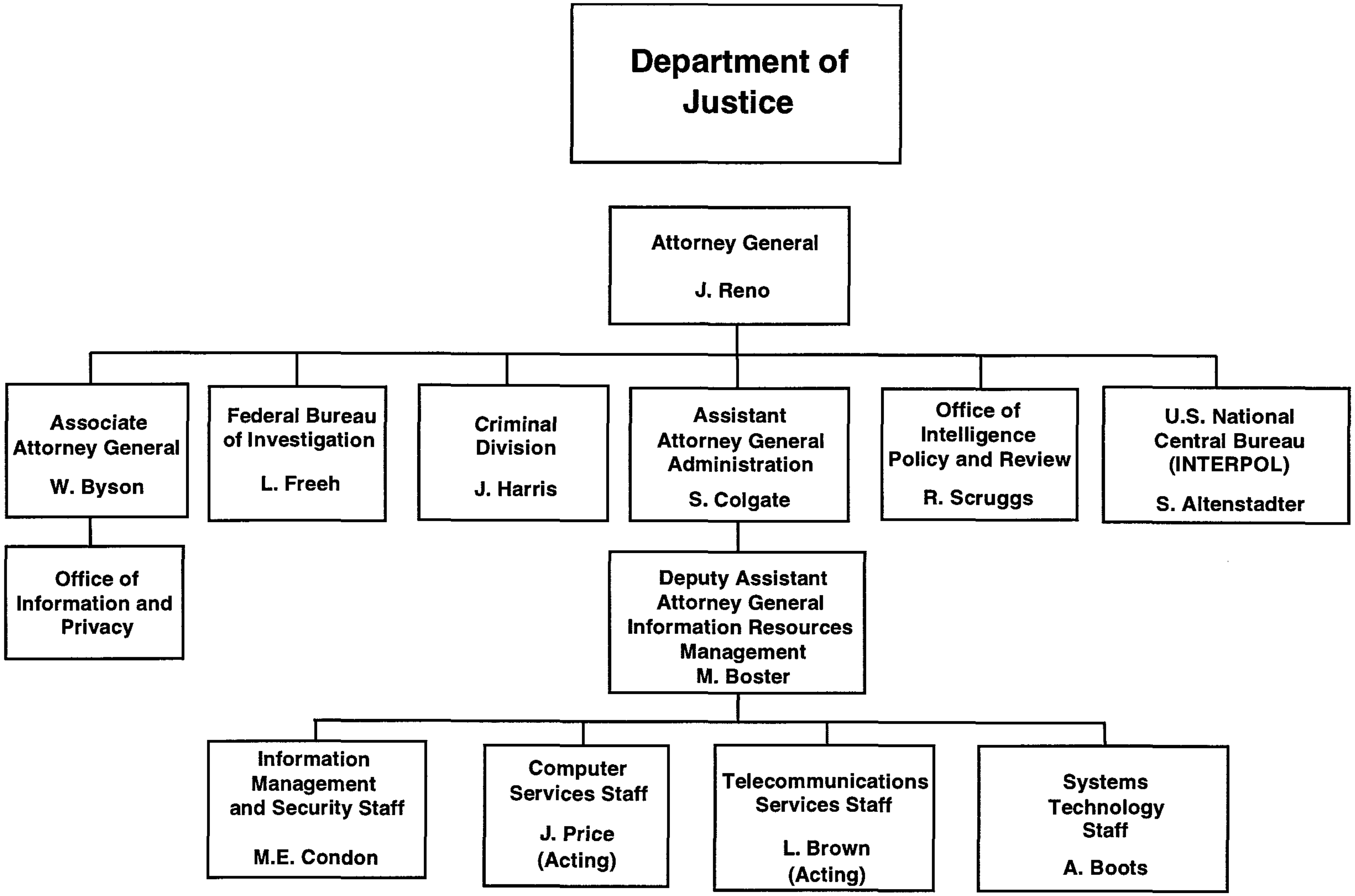
SNL Homepage: http://www.sandia.gov/

Information Assurance Related Missions and Functions:

The end of the Cold War era has stimulated DOE's national laboratories to contribute to economic security, synergistic with their public missions in defense, energy, and the environment. Recognizing the complexity of the issues and relationships for industry-led and government partnered enterprises, Sandia's National Industrial Alliances Center has developed and implemented the Prosperity Games in partnership with the National War College, Lawrence Livermore National Laboratories, the Electronics Industries Association, and the American Electronics Association. Under the auspices of the Electronics Subcommittee of the NSTC, the Prosperity Games have provided energy for and assessment of road maps of the technology and policy options related to electronic manufacturing in the United States.

Information Assurance Activities, Issues, Best Practices, Lessons Learned:

- The Sandia National Laboratories are engaged in a joint effort with the Los Alamos National Laboratory and the Lawrence Livermore National Laboratory to develop a real-time intrusion detection and response system that can supplement or complement an information assurance program for protecting the Department's information resources.
- The Sandia National Laboratories are also heavily involved in a broad range of authentication and encryption topical areas in addition to information surety, firewall architecture, data base design and implementation, and educational delivery methodologies and mechanisms.


Department of Justice
Attorney General
J. Reno
Associate Attorney General
W. Byson
Office of Information and Privacy
Federal Bureau of Investigation
L. Freeh
Criminal Division
J. Harris
Assistant Attorney General Administration
S. Colgate
Office of Intelligence Policy and Review
R. Scruggs
U.S. National Central Bureau (INTERPOL)
S. Altenstadter
Deputy Assistant Attorney General Information Resources Management
M. Boster
Information Management and Security Staff
M.E. Condon
Computer Services Staff
J. Price (Acting)
Telecommunications Services Staff
L. Brown (Acting)
Systems Technology Staff
A. Boots

Organization: Department of Justice (DoJ)

Senior Information Assurance Official:

Stephen R. Colgate, Assistant Attorney General For Administration

Information Assurance Points of Contact:

Mark A. Boster, Deputy Assistant Attorney General for Information Resources Management (IRM)
Mary Ellen Condon, Director, Information Management and Security Staff (IMSS), IRM
Scott Charney, Chief, Computer Crime Unit, Criminal Division
Robert Bryant, Assistant Director, National Security Division, FBI
Neil J. Gallagher, Deputy Assistant Director, Criminal Investigative Division, FBI

On-Line Resources:

DoJ Homepage: http://www.usdoj.gov/
Federal Bureau of Investigation: http://www.fbi.gov/
FBI National Computer Crime Squad: http://www.fbi.gov/compcrim.htm
Drug Enforcement Agency: http://www.usdoj.gov/dea/deahome.htm

Information Assurance Related Missions and Functions:

The Department of Justice serves as counsel for the Nation's citizens. It exercises this primary responsibility through law enforcement, crime prevention, crime detection, prosecution, incarceration, and rehabilitation of offenders.

The Office of Information and Privacy coordinates policy development and Government-wide compliance with the Freedom of Information and Privacy Acts.

The Justice Management Division (JMD) provides assistance to senior management officials concerning basic departmental policy for automatic data processing, telecommunications, security, and records management, as well as budget and financial management, personnel management and training, equal opportunity programs, procurement, real property and materiel management, and for all other matters pertaining to organization, management and administration. JMD develops and disseminates policies, standards and procedures for managing automated information processing resources. JMD also reviews the implementation of these policies, standards and procedures. In addition, JMD provides automated litigation support, and collects, organizes, and disseminates recorded information that is necessary to the DoJ in carrying out its statutory mandates.

The Office of Intelligence Policy and Review advises the Attorney General on national security matters. The office prepares and files applications for surveillance under the Foreign Intelligence Surveillance Act of 1978 and advises all Government agencies on national security law.

The Antitrust Division is responsible for promoting and maintaining competitive markets by enforcing the Federal antitrust statutes and by acting as an advocate of competition within the Federal government. The division also represents the United States in judicial proceedings to review certain orders of regulatory bodies such as the Federal Communications Commission.

The Criminal Division develops, enforces and supervises the application of all Federal criminal statutes, except those specifically assigned to other divisions. The division includes the Fraud Section that directs and coordinates the Federal effort against fraud and white collar crime; the Internal Security Section that supervises the investigation and prosecution of cases affecting the national security, foreign relations, and the export of military and strategic commodities and technology; and the Money Laundering Section. Also included it the Computer Crime Unit, which is responsible for implementing the Computer Crime Initiative, a five-point program that is designed to respond to the mounting computer crime problem.

DoJ takes a keen interest in investigating and prosecuting computer crimes ranging from intrusions prosecuted under Title 18 USC § 1030 to communication of threats over networks. DoJ is interested not only in crimes directed against DoJ facilities but in all violations of Federal law. for example, DoJ works closely with the Air Force's Office of Special Investigations and other military components to address attacks against military computer systems.

The Federal Bureau of Investigation is the principal investigative arm of the Department. At present, organized crime/drugs, counterterrorism, white collar crime, foreign counterintelligence, and violent crime are the Bureau's investigative priorities. The Economic Crime Unit in the White Collar Crime Section of the Criminal Investigative Division has primary responsibility for computer crime investigations.

The United States National Central Bureau represents the United States in the International Criminal Police Organization (INTERPOL). The National Central Bureau provides an essential communications link between the U.S. police community and their counterparts in foreign member countries.

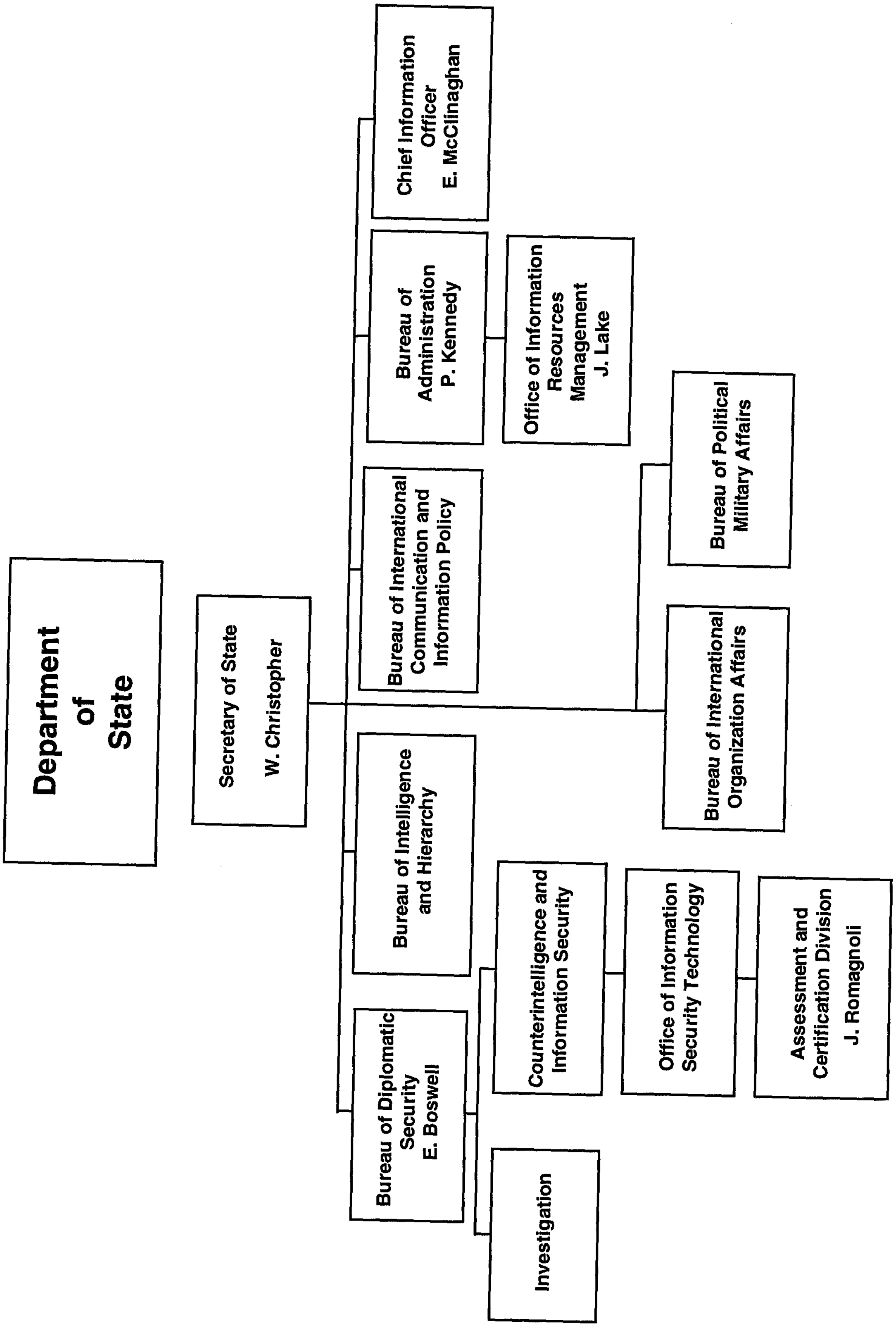
Information Assurance Activities, Issues, Best Practices, Lessons Learned:

- The Department has formed a Computer Security Officers Task Force consisting of the representatives with computer security responsibility from each of the Departments 34 components. Each component Computer Systems Program Manager is responsible for overseeing the activities of Computer Systems Security Officers designated for each system. These systems security officers are full-time or part-time security specialists, depending on the size and sensitivity of the system and its information.
- The Department has unique information protection requirements. On one hand it is obligated to share its information with the public and other law enforcement agencies. On the other, the information held at the Department, such as evidence and fingerprints, is very sensitive information. In addition, DoJ must share considerable information with the Judiciary.
- Since DoJ is the principal agency responsible for the Federal government's litigation and law enforcement functions, many critical systems and services could be affected: immigration and border controls; criminal investigations; civil suits, many involving large sums of money; control of the Federal prison system; litigation and settlements in antitrust cases; litigation of criminal and civil tax cases; matters involving environmental laws; and many others. Specifically in the area of national security, the Department handles many sensitive matters involving intelligence information, including wiretaps under the Foreign Intelligence Surveillance Act; FBI counterintelligence investigation; and liaison operations of the FBI, Drug Enforcement Agency and others in foreign countries.
- DoJ is in the midst of proposing legislation to further strengthen the laws available to prosecutors in the high-technology area (Title 18 U.S.C. § amendments, copyright provisions, Privacy Protection Act, etc.).
- The Criminal Division coordinates closely with many other components, such as the FBI National Computer Crime Squad and the FBI Computer Analysis and Response Team, to exchange information and develop better legal and tactical approaches to computer crimes. DoJ also coordinates with the Secret Service, IRS, Air Force, Navy, and others.
- Each U.S. Attorney's Office designates a Computer/Telecommunications Coordinator. These coordinators are prosecutors who receive special training in technology issues to act as the central point of contact who understands technical matters.
- Information protection is accomplished by risk management, which includes estimates of the viability of the threat and value of the information that must be protected. The threat is a validated threat produced at DoJ. Of note, private detectives and skip tracers (people who located others persons who default on bail, loans, etc.) constitute a significant threat to DoJ information, as do organized crime, drug trafficking, etc. Additional considerations include the distribution of information and the data upon which the information is based and the aggregation of information.
- Two projects represent DoJ best practices in information protection: the Counternarcotics Information Sharing Project and the Joint Automated Booking System. The Counternarcotics Information Sharing Project, sometimes referred to as Drug X, is an information pointer system that was developed in a cooperative manner with two components and was based upon extensive discussions with the users. Developing the system involved developing an architecture based on multiple platforms and information

protection requirements. The Joint Automated Booking System was developed by five DoJ components.

- The Department's Justice Performance Review Office recently received approval to establish a Computer Security Technical Laboratory, which will include a DoJ Incident Response Service (DOJIRS) and an advanced authentication and encryption test bed.
- Information security policy oversight for unclassified DoJ systems is conducted by the IMSS. The basis for policy is the existing body of laws and regulations regarding matters with which the various components of DoJ must deal. IMSS relies on the DoJ components to provide legal advice and assistance. The staff translates the laws and regulations into technical policy which is then disseminated to the components. components also write implementing policy which the IMSS periodically reviews for compliance with higher level policy. The policy is also based on existing Executive Branch policy and standards to include NIST standards where applicable. In general, existing technical policy is centered on the goal of C2 level of protection of information. Implementation of the policy is also complicated by legacy systems and rapid changes in technology.
- There are now four staffs instead of five under the Deputy Assistant Attorney General for IRM, Mark A. Boster. The Computer and Telecommunications Security Staff (CTSS) and the Systems Policy Staff were combined to form the Information Management and Security Staff (IMSS), headed by Mary Ellen Condon. IMSS has responsibility for all the policy and security functions that were handled by CTSS in the past.
- The FBI is expanding its outreach program to industry, known as Development of Espionage, Counterintelligence and Counterterrorism Awareness (DECA) program, to include a communications network to inform corporations of industrial spying and technology transfer threats and to provide defensive tips. The Bureau plans to include computer crimes against industry in the information to be addressed.
- The FBI and the Secret Service have formed a coordination group with several banking associations to combat financial fraud and computer crimes. The banking associations include the Washington-based American Bankers Association, Independent Bankers of America, America's Community Bankers, and the Credit Union National Association. [Washington Technology, May 23, 1996, page 8]

This page intentionally left blank.


Department of State
Secretary of State W. Christopher
Chief Information Officer E. McClinaghan
Bureau of Administration P. Kennedy
Office of Information Resources Management J. Lake
Bureau of International Communication and Information Policy
Bureau of Political Military Affairs
Bureau of International Organization Affairs
Bureau of Intelligence and Hierarchy
Bureau of Diplomatic Security E. Boswell
Counterintelligence and Information Security
Office of Information Security Technology
Assessment and Certification Division J. Romagnoli
Investigation

Organization: Department of State (DoS)

Senior Information Assurance Official:

Eric Boswell, Assistant Secretary for Diplomatic Security

Information Assurance Points of Contact:

Eliza McClenaghan, Chief Information Officer
Joseph Lake, Deputy Assistant Secretary for Information Management
Jules Romagnoli, Chief, Assessment and Certification Division, Bureau of Diplomatic Security

On-Line Resources:

DoS Homepage: http://www.whitehouse.gov/WH/Cabinet/html/Department_of_State.html

Information Assurance Related Missions and Functions:

The Department of State advises the President in the formulation and execution of foreign policy. The Department's primary objective in the conduct of foreign relations is to promote the long-range security and well-being of the United States.

The Secretary is the first ranking member of the Cabinet and a member of the National Security Council. The Under Secretary for International Security Affairs is responsible for assuring the integration of all elements of the Foreign Assistance Program and serves as the Chairman of the Arms Transfer Management Group. The Under Secretary is also responsible for international scientific and technological issues, communications and information issues, and technology transfers.

The Bureau of Diplomatic Security provides a secure environment for conducting American diplomacy and promoting American interests worldwide. It assists the Secretary in the formulation and implementation of diplomatic security policy to provide a secure environment for the conduct of American diplomacy and coordinates the exchange of security-related intelligence and operational information among the Department, foreign governments, other U.S. Government agencies, and all law enforcement authorities. The Bureau provides administrative support to the Overseas Security Advisory Council, a Federal Advisory Committee, which provides for regular and timely exchange of information between the private sector and the Department.

The Bureau of Intelligence and Research coordinates the programs of intelligence, analysis, and research and produced intelligence studies and current intelligence analyses.

The Bureau of International Communications and Information Policy coordinates with other U.S. Government agencies and the private sector in the formulation and implementation of international policies relating to a wide range of rapidly evolving communications and information technologies. The Bureau also promotes U.S. telecommunications interests bilaterally and multilaterally.

The Bureau of International Organization Affairs leads in the development, coordination, and implementation of U.S. multilateral policy. It formulates and implements U.S. policy toward international organizations with particular emphasis on those organizations which make up the United Nations system.

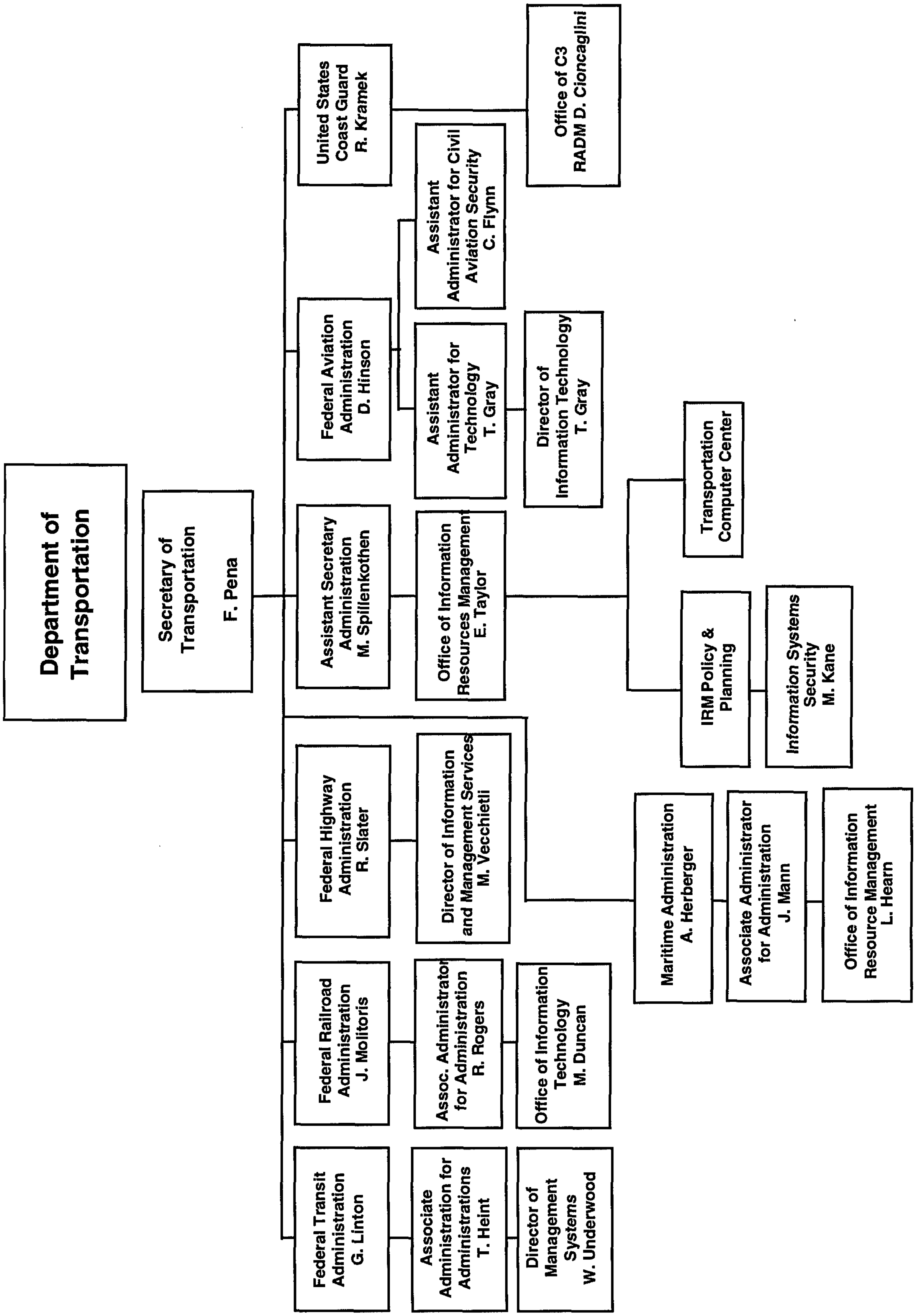
The Bureau of Political-Military Affairs coordinates policy formulation on national security issues including defense relations and security assistance and export controls. The Bureau's major activities are designed to further U.S. national security objectives by through negotiations, security assistance, curbing proliferation of weapons of mass destruction, and inhibiting adversaries access t military significant technologies.

Information Assurance Activities, Issues, Best Practices, Lessons Learned:

- The Under Secretary for Management has directed the Assistant Secretaries to take responsibility for security of systems under their direction.
- Bureau of Diplomatic Security develops and promulgates security policy with the involvement of the other DoS bureaus. Office of Information Security Technology drafts the policy. Office includes responsibility for records security (Ms. Mary Stone) which includes damage assessment and classification of information.
- DS/CIS participates in the NSTISSC. The Deputy Assistant Secretary for CIS is the DoS representative to NSTISSC. Chief, Assessment and Certification Division is the DoS representative to the SAIS and the STSS.
- Operational communications matters are responsibility of Office of Information Management in the Bureau of Administration. Although Office of Information Management and OIST are in different bureaus, they work closely to integrate security early in the systems development process.
- Security policies are articulated in Foreign Affairs Manual.
- The Department is beginning to emphasize risk management. Some savings have already been achieved by moving to risk management. Also trying to identify responsibilities for Assistant Secretaries and pin point ownership of information.
- Assurance goals are always mitigated by operational considerations.
- Major issues are how to incorporate security in open systems architectures, multilevel security, logical management architectures, and networks. Another issue is the fast-paced introduction of technology which seems to out pace the introduction of security technologies. Also need a standard mechanism for sharing information.
- DoS will use DoD Defense Messaging System -- saves on development. DoS does not do any research and development.
- DoS does, however, operate a computer security laboratory which is configured as a model embassy. The lab is used to test security policies before implementation. The lab

simulates overseas operations for security certification of systems and software. The lab budget is approximately $1.5 million per year. Computer security laboratory used to test, assess, and evaluate security methods. Firewalls used but limit capabilities. Encryption also used but with associated limitations (commonality of equipment, key distribution, limited access, information constraining).

- OIST's education and awareness training are oriented on operational matters, not mandatory security training issues.
- As a result of a recent *Wall Street Journal* article, DoS representatives expect to be called to testify before the Senate Permanent Subcommittee on Investigations which is holding hearings on computer security.
- OIST recently completed a risk management study on providing Internet access to DoS employees. While the business case for Internet access has not been fully developed, the risks associated with several options (desktop, stand-alone, separate network) to providing the service have been fully identified and briefed to management personnel.
- DoS is developing a response plan for computer emergencies. The plan calls for decentralized implementation and is oriented on intrusions from the Internet and viruses. The plan has not yet been fully exercised.
- DoS develops its own tools and procedures to evaluate its systems and networks. These evaluations are conducted based on network complexity, perceived threats, and system and network improvements.
- The Under Secretary for Management and the Chief Information Officer are very knowledgeable of the security risks and have been very supportive of the security programs. For example, the Under Secretary manages a program in which the Bureaus compete for money to support Bureau initiatives which have department-wide value. Approval of a program initiative is contingent on a security approval by OIST and six percent of the program funds must be devoted to security (requirements definition and implementation). A recently approved program has resulted in the electronic delivery of classified and unclassified telegrams employing a from of multilevel security.
- Budget and staffing for information security have remained stable. Some additional funding (nearly 50%) has been made available this fiscal year because of management interest in security initiatives.
- The Office of Information Management has formed a team to define the DoS information infrastructure. Several foundations (e.g., security, configuration management, training) are being established before the infrastructure is defined in detail. It is envisioned that these foundations will lead to standardization and interoperability.
- OIST personnel are devoting special attention to integrity and availability issues.


Department of Transportation
Secretary of Transportation
F. Pena
United States Coast Guard
R. Kramek
Office of C3
RADM D. Cioncaglini
Federal Aviation Administration
D. Hinson
Assistant Administrator for Civil Aviation Security
C. Flynn
Assistant Administrator for Technology
T. Gray
Director of Information Technology
T. Gray
Assistant Secretary Administration
M. Spillenkothen
Office of Information Resources Managemen
E. Taylor
Transportation Computer Center
IRM Policy & Planning
Information Systems Security
M. Kane
Federal Highway Administration
R. Slater
Director of Information and Management Services
M. Vecchietti
Maritime Administration
A. Herberger
Associate Administrator for Administration
J. Mann
Office of Information Resource Management
L. Hearn
Federal Railroad Administration
J. Molitoris
Assoc. Administrator for Administration
R. Rogers
Office of Information Technology
M. Duncan
Federal Transit Administration
G. Linton
Associate Administration for Administrations
T. Heint
Director of Management Systems
W. Underwood

Organization: Department of Transportation (DoT)

Senior Information Assurance Official:

Mellisa J. Spillenkothen, Assistant Secretary for Administration

Information Assurance Points of Contact:

Michael Kane, DoT Information Systems Security Officer, Office of Information Resource Management

On-Line Resources:

DoT Homepage: http://www.dot.gov
FAA: http://www.faa.gov
FAA Technical Center: http://www.tc.faa.gov/

Information Assurance Related Missions and Functions:

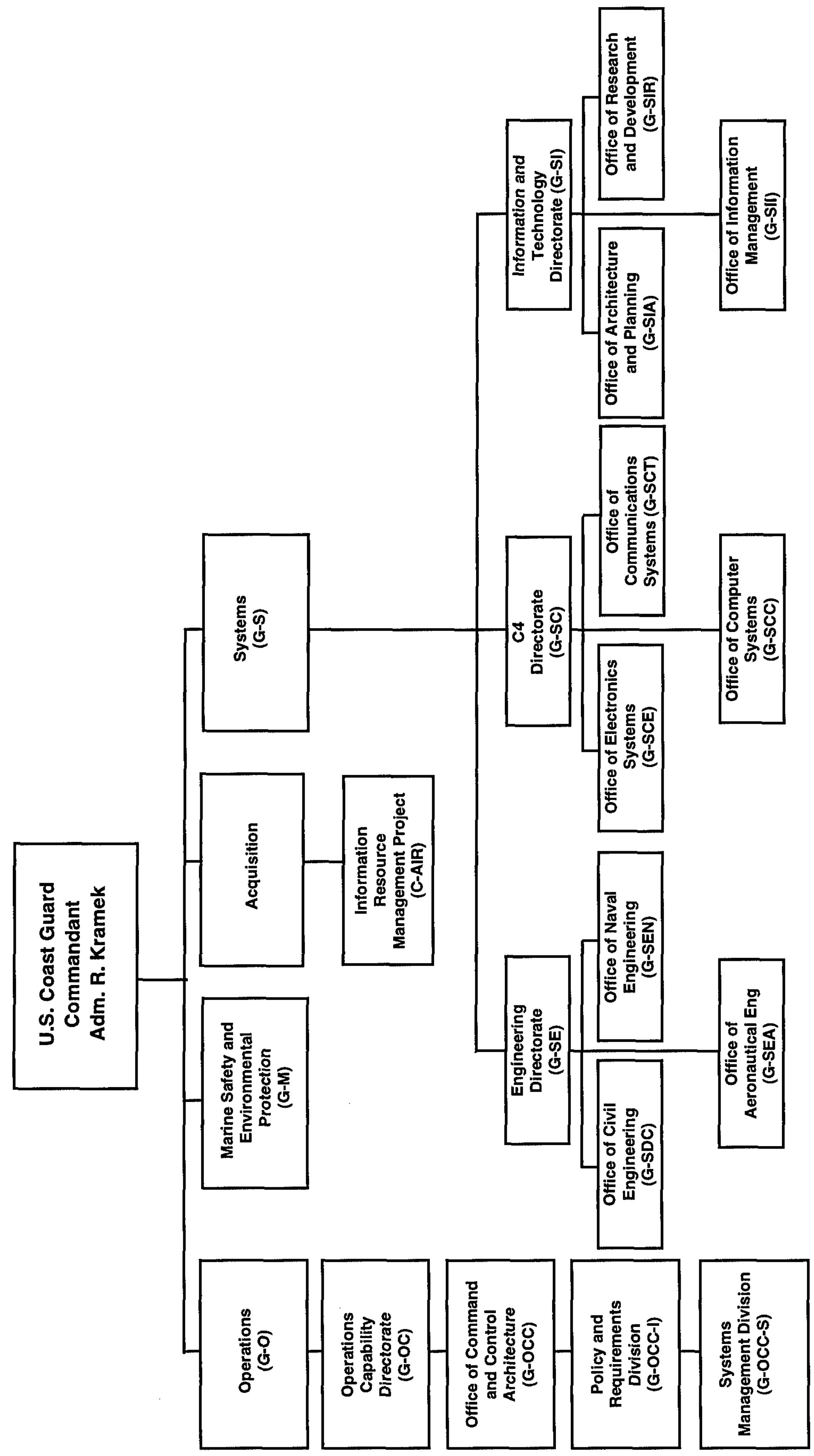
The Office of Information Resource Management formulates, prescribes, and assures compliance with telecommunications and automated data processing policy to include information systems security policy.

Information Assurance Activities, Issues, Best Practices, Lessons Learned:

- The Departmental Information Systems Security Officer is supported by a staff of two people. Budget is very limited. U.S. Coast Guard (USCG). has three information security staff personnel supported by nine regional officers who perform information security duties as collateral duties. Federal Aviation Administration (FAA) has two information security staff personnel supported by ten regional officers who perform information security duties as collateral duties. Computer centers (Washington, DC, Plano, TX, Cambridge, MA) have full time security officers.
- Reinvention of DoT may result in:
  - Reduction of operating administrations to three -- FAA, USCG, Intermodal Transportation Agency (ITA)
  - Reduction in employees from 105,000 to 50,000 (Including military)
  - Reduction in grant programs from 30 to 3
  - Privatization of air traffic control activities
- Traditional security concerns in DoT have focused more on keeping planes in the air vice information security.
- Reduction in grant programs will be accompanied by establishment of "Transportation Banks" for disbursement of moneys. This will add enormous security requirements regarding electronic commerce and electronic funds transfer. DOTreas is providing advice on related issues.

- Senior official for information systems security is the Assistant Secretary for Administration, who chairs an Advisory Management Committee (AMC). The Executive Agent for Information Security is Eugene Taylor, the Director of Information Resource Management, who chairs the IRM Advisory Committee (IRMAC). Mr. Kane, the Departmental Information Systems Security Officer, chairs the Subcommittee on Computer Security (SOCS). The AMC and the IRMAC have membership from the operating administrations. The SOCS has membership from the operating administrations, the Inspector General's Office, and the Computer Centers.
- DoT has been actively conducting oversight reviews to improve security posture. Two years ago, only two of ten operating administrations had information security policies. Will actively continue the reviews, some in the form of self assessments.
- Reviews resulted in establishment of a very good training and awareness program which has been very effective at the end-user level. Still need a similar program to influence management. Will address all OPM and procurement categories and establish performance areas for executives, senior functional managers, IRM personnel, and security personnel.
- DoT uses a departmental security banner on all systems. Also employs a user authorization form for every user.
- Growth of electronic commerce may outrun our ability to adequately secure the commerce. Help from GSA (responsible for the security infrastructure) slow in coming.
- DoT has completed extensive policy-to-standards translations.
- Intend to do penetration demonstration for senior managers in near future.
- DoT concerned about whether significant employee reductions will increase insider threat.
- Mr. Kane thinks the Federal Computer Security Program Manager's Forum is productive.
- Information security issues:
  - Multiple e-mail protocols and associated problems.
  - Reinvention of DoT means a new corporate architecture.
  - Which encryption schemes to use (hardware, software, embedded, digital signature standard).
  - Use of conformance standards and how to couple with controls.
- Security must be cost effective and consistent with information being protected. Simple quick-fix, low cost solutions are available.
- Have experienced several penetrations. In one instance, the Intermodal LAN was penetrated within hours of its activation. The perpetrator used the LAN to weave to Maryland and Virginia banks and other sensitive operations.
- The Office of Information Resources Management is in the process of establishing the Information Technology Omnibus Procurement, a multi-year, multiple award contract valued at over $1 billion which will be used to provide information systems engineering, facilities management, and systems security services to the entire department on a fee-for-service basis. It is expected that awards will be made by October 1, 1996.
- The budget for information technology (including information systems security) is shrinking.

This page intentionally left blank.


U.S. Coast Guard
Commandant
Adm. R. Kramek
Operations (G-O)
Marine Safety and Environmental Protection (G-M)
Acquisition
Systems (G-S)
Information Resource Management Project (C-AIR)
Operations Capability Directorate (G-OC)
Office of Command and Control Architecture (G-OCC)
Policy and Requirements Division (G-OCC-I)
Systems Management Division (G-OCC-S)
Engineering Directorate (G-SE)
Office of Civil Engineering (G-SDC)
Office of Naval Engineering (G-SEN)
Office of Aeronautical Eng (G-SEA)
C4 Directorate (G-SC)
Office of Electronics Systems (G-SCE)
Office of Communications Systems (G-SCT)
Office of Computer Systems (G-SCC)
Information and Technology Directorate (G-SI)
Office of Architecture and Planning (G-SIA)
Office of Research and Development (G-SIR)
Office of Information Management (G-SII)

Organization: United States Coast Guard (USCG)

Senior Information Assurance Official:

RADM John Tozzi, Director, Information and Technology Directorate (G-SI)

Information Assurance Points of Contact:

CAPT Dave Potter, C4 Directorate, Systems
CAPT Dick Mead, Office of Command and Control Architecture, Operations
LCDR Mike Inman, Office of Command and Control Architecture, Operations
CAPT Ben Chiswell, Office of Communications Systems, C4 Directorate, Systems
CDR Mike Grimes, Office of Communications Systems, C4 Directorate, Systems

On-Line Resources:

USCG Homepage: http://www.dot.gov/dotinfo/uscg/

Information Assurance Related Organizations, Missions and Functions:

USCG missions include: Maritime Search and Rescue, Ice Operations and Marine Science Activities, Commercial Vessel Safety, Marine Environmental Protection, Port Safety and Security, Maritime Law Enforcement/Enforcement of Laws and Treaties, Contingency Preparedness/Defense Operations and Recreational Boating Safety. It is subordinate to the Navy during time of national emergency.

The Director of the Information and Technology Directorate (G-SI) is the USCG Chief Information Officer. Primary responsibility for information security policy lies with the Office of Information Management (G-SII) in G-SI.

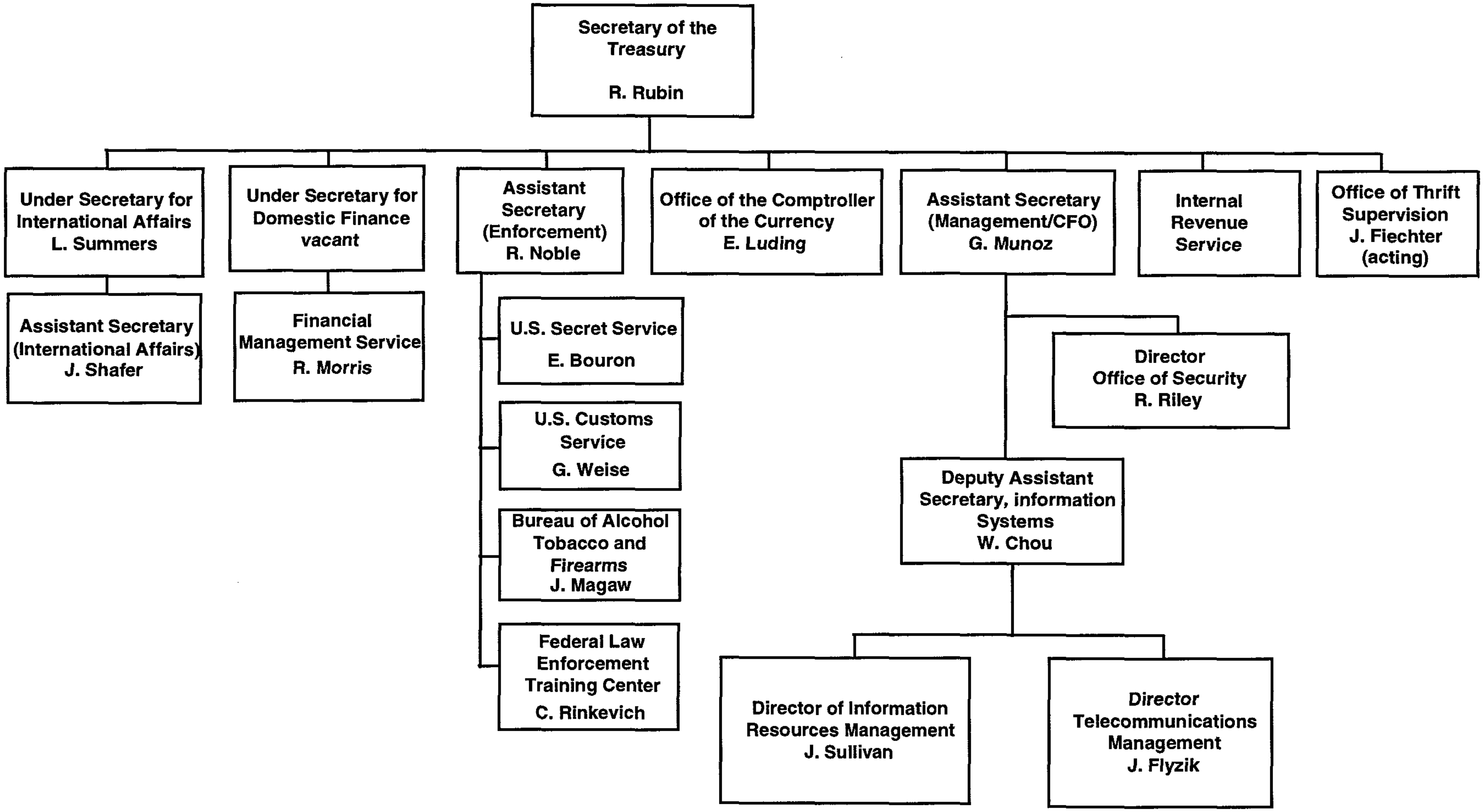
Information Assurance Activities, Issues, Best Practices, Lessons Learned:

- With respect to IW, the biggest issue for the Coast Guard is interoperability. Standard operations for the Coast Guard do not mirror DoD when it comes to standardized equipment, procedures, communications assets, or communications paths. The Coast Guard has limited access to MILSATCOM, but current bandwidth does not fulfill data requirements. Navy and Coast Guard have similar information requirements, especially when operating jointly. Near real-time requirements for unique missions have forced the Coast Guard to seek commercial satellite alternatives.
- The Coast Guard supports national security interests but not in the same sense as DoD. The Coast Guard has no organizational definition of IW, and even if it did, it is likely it would differ from the DoD definition. An example of a national security interest which directly involves the Coast Guard is the migrant issue. Migrants are an issue to the State Department, but is not as identifiable with DoD.

- Another key issue which distinguishes the Coast Guard from DoD is the origination of classified information. The Coast Guard has limited authority to originate classified information. Most classified information handled by the Coast Guard is derivative in nature. However, most information on Coast Guard unique missions (Maritime Law Enforcement, Search and Rescue, etc.) can be handled at the unclassified but sensitive level.
- The Coast Guard is developing a C4I architecture which will encompass all aspects of C4I and sensors.
- The Coast Guard is planning full migration to the Defense Message System (DMS). The transition plan is currently under development.

This page intentionally left blank.

Department of the Treasury



Secretary of the Treasury

R. Rubin

Under Secretary for International Affairs
L. Summers

Assistant Secretary (International Affairs)
J. Shafer

Under Secretary for Domestic Finance
vacant

Financial Management Service
R. *Morris*

Assistant Secretary (Enforcement)
R. Noble

U.S. Secret Service

E. Bouron

U.S. Customs Service

G. Weise

Bureau of Alcohol Tobacco and *Firearms*
J. Magaw

Federal Law Enforcement Training Center

C. Rinkevich

Office of the Comptroller of the Currency
E. *Luding*

Assistant Secretary (Management/CFO)
G. *Munoz*

Director
Office of Security
R. Riley

Deputy Assistant Secretary, information Systems
W. Chou

Director of Information Resources Management
J. Sullivan

Director
Telecommunications Management
J. Flyzik

Internal Revenue Service

Office of Thrift Supervision
J. Fiechter
(acting)

Organization: Department of the Treasury (Treas)

Senior Information Assurance Official:

G. Munoz, Assistant Secretary for Management and Chief Financial Officer

Information Assurance Points of Contact:

R. Riley, Director, Office of Security
M. Ferris, Systems Security, Office of Security
W. Chou, Deputy Assistant Secretary for Information Systems
J. Sullivan, Director, Office of Information Resources
J. Flyzik, Director, Office of Telecommunications Management

On-Line Resources:

DoTreas Homepage: http://www.ustreas.gov/treasury/Homepage.html
U.S. Secret Service: http://www.ustreas.gov/treasury/bureaus/usss/usss.html
FinCen: http://www.ustreas.gov/treasury/bureaus/fincen/fincen.html
US Customs Service: http://www.ustreas.gov/treasury/bureaus/customs/customs.html

Information Assurance Related Missions and Functions:

The Department of the Treasury formulates and recommends domestic and international economic, financial, tax, and fiscal policies; serves as financial agent of the U. S. Government; enforces Federal statutes; and manufactures coins and currency.

The Secretary serves as the Chief Financial Officer of the U. S. Government, Chairman *pro tempore* of the Economic Policy Council and as U. S. Governor of the International Monetary Fund and the International Bank for Reconstruction and Development, as well as the Inter-American and African Development Banks.

The Assistant Secretary (Enforcement) supervises the Bureau of Alcohol, Tobacco and Firearms (BATF); Federal Law Enforcement Training Center (FLETC); United States Customs Service (USCS); and the United States Secret Service (USSS) and the Financial Crimes Enforcement Network (FinCEN). The Assistant Secretary (Enforcement) is also responsible for the Office of Financial Enforcement and the Office of Foreign Assets Control.

- Aside from the Presidential protection mission, the USSS is responsible for White House security and the security of foreign missions in the United states. The USSS also enforces statutes related to currency, coins, obligations, and securities of the United States and foreign governments; forgery or fraudulent negotiation of Federal government checks, bonds, and other obligations or securities of the United States; criminal violations of the Federal Deposit Insurance Act; electronic funds frauds, credit and debit card frauds, false identification documents or devices, computer access fraud, and U. S. Department of Agriculture food coupons; and others

.

- The USCS collects the revenue from imports and enforces customs and related laws, such as export and technology transfer statutes.

- The BATF enforces and administers firearms and explosives statutes, as well as the statutes concerning producing, taxing and distributing alcohol and tobacco products.

- FLETC provides training for the Department of Treasury. This training is also available to other Federal, state and local police agencies.

The Financial Crimes Enforcement Network (FinCEN) provides a Government-wide, multi-source intelligence and analytical network to support other agencies in detecting, investigating and prosecuting domestic and international money laundering and other financial crimes. FinCEN provides law enforcement with tactical and strategic intelligence analyses that identify emerging trends and geographical patterns of money laundering and suspected offenders. FinCEN provides specially trained investigators who are experienced in analyzing financial records and data and operates a communications center to answer requests from law enforcement agencies for specific data and information.

The Undersecretary of Domestic Finance supervises the administration of the Government's fiscal affairs including administrating Treasury financing operations; managing Treasury's cash balances in tax and loan investment accounts in commercial financial institutions, as well as the operating balances of Federal Reserve Banks; and participating in the Joint Financial Management Improvement Program for improving accounting in the Federal government.

- The Financial Management Service provides financial services, information and advice to the Treasury Department, Federal program agencies and Government policy makers. The Service issues Treasury checks and electronic fund transfer payments to meet the Federal payroll, social security, veteran's benefits, and income tax refunds.

- The Bureau of Public Debt borrows the money needed to operate the Federal government; accounts for the public debt; and issues Treasury securities to refund maturing debt and raise new money.

The Assistant Secretary (International Affairs) advises the Secretary on international monetary, financial, commercial, energy, and trade policies and programs.

The Internal Revenue Service (IRS) administers internal revenue statutes and educates the public as to their rights and responsibilities under these laws.

The Office of the Comptroller of the Currency regulates national banks. This office examines banks and has the power to close banks that are not in compliance. The office also issues rules and regulations.

The Office of Thrift Supervision charters and regulates Federal- and State-chartered thrift institutions belonging to the Savings Association Insurance Fund.

The Inspector General is responsible for providing comprehensive, independent and objective audit and investigation programs to identify and report program deficiencies and improve the economy, efficiency and effectiveness of operations.

The Treasurer of the United States oversees the U. S. Mint and the Bureau of Engraving and Printing. The primary mission of the Mint is to produce an adequate volume of circulating coinage for the Nation to conduct its trade and commerce. The Bureau of Engraving and Printing designs, prints and finishes a wide range of security products, to include Federal Reserve notes, U. S. postage stamps, Treasury securities, identification cards, and certificates. This bureau also assists other Federal agencies in designing and producing documents that require some level of security or counterfeit-deterrence.

Information Assurance Activities, Issues, Best Practices, Lessons Learned:

- The Department of the Treasury has approximately 165,000 employees and operates in a decentralized manner. It relies on OMB and GSA guidance for security of sensitive unclassified information.
- Training alone may not be a cost-effective means of improving security.
- The information assurance discussion seems to focus on the vulnerability of telecommunications, but should also be concerned about value-added networks that serve as additional communications infrastructure and which ride on the telecommunications infrastructure.
- The A-130 policy seems to imply that the policy should be "let the buyer beware," and although there may be some merit in this approach, policy should also establish minimum standards. The Department of the Treasury participates in several *ad hoc* efforts to develop standards.
- The Department, with input from departmental security experts, writes very broad policy for internal implementation. Minimum standard practices are included in the Department's security manual.
- As seems to be the case Government-wide, there is not much budget available for security efforts.
- The Department is establishing a very extensive communications and data network, the Treasury Communications System, which will rely on commercial telecommunications.
- The Department does not conduct active penetration testing of the Department's networks. Some Bureaus, such as the IRS, do conduct tests of their own networks.
- The Department continues to be involved in a substantial amount of computer crime investigations. Bob Friel, Financial Crimes, can provide details.

- The Office of the Comptroller of the Currency regulates national banks, the Federal Deposit Insurance Corporation regulates certain banking operations. FEDline is a computer-to-computer encrypted system used for transfers from government activities to the Federal Reserve System (FRS).
- The Department's Telecommunications and Information Security Working Group coordinates information security issues. Information systems security officers conduct certification and accreditation. Security duties included in job descriptions and categories identify personnel who are qualified or experienced in security of specific systems or classes of systems.
- The Department, IRS and Financial Management Service participate in developing banking standards.
- Wireless architecture and security issues are being addressed by the USSS.
- The USSS is continuing to participate in Joint Computer Crime Unit activities. The unit recognizes that hackers share information and tools in the global village that in the hands of a person with malicious intent could be used to cause grave damage to US interests. The unit hopes to preempt such attacks and shares its information in an interagency forum.
- The USSS commented that over the last year there has been a rise in the percentage of outsider attacks on industry versus insider. The proportion is now approximately 40 percent outsider versus 60 percent insider attacks.
- The Secret Service and the FBI have formed a coordination group with several banking associations to combat financial fraud and computer crimes. The banking associations include the Washington-based American Bankers Association, Independent Bankers of America, America's Community Bankers, and the Credit Union National Association. [Washington Technology, May 23, 1996, page 8]

Interagency Groups

Interagency Groups

This page intentionally left blank.

Federal Agency Computer Security Program Managers' Forum

Co-Chairs
S. Pitcher, DoC
E. Roback, NIST

Organization: Federal Agency Computer Security Program Managers' Forum

Senior Information Assurance Official:

Information Assurance Points of Contact:

Sadie Pitcher, Department of Commerce, Co-Chair
Ed Roback, National Institute of Standards and Technology, Co-Chair

On-Line Resources:

Information Assurance Related Missions and Functions:

The Federal Agency Computer Security Program Managers' Forum sponsored by NIST is an informal government interagency organization for advocacy and information exchange on computer security issues among Federal departments and agencies. The Federal Agency Computer Security Program Managers' Forum addresses issues related to the security of unclassified federal computer and telecommunications systems (except "Warner Amendment" systems as described in 44 U.S.C. Section 3502).

The Managers' Forum has no legal or regulatory basis as such, but rather, was created out of need by NIST. The Managers' Forum is mainly an information-sharing body, though its charter was recently changed to make it into a more proactive group.

Membership includes the following organizations. Where a subordinate organization is indicated, both the parent and subordinate organizations may join as members.

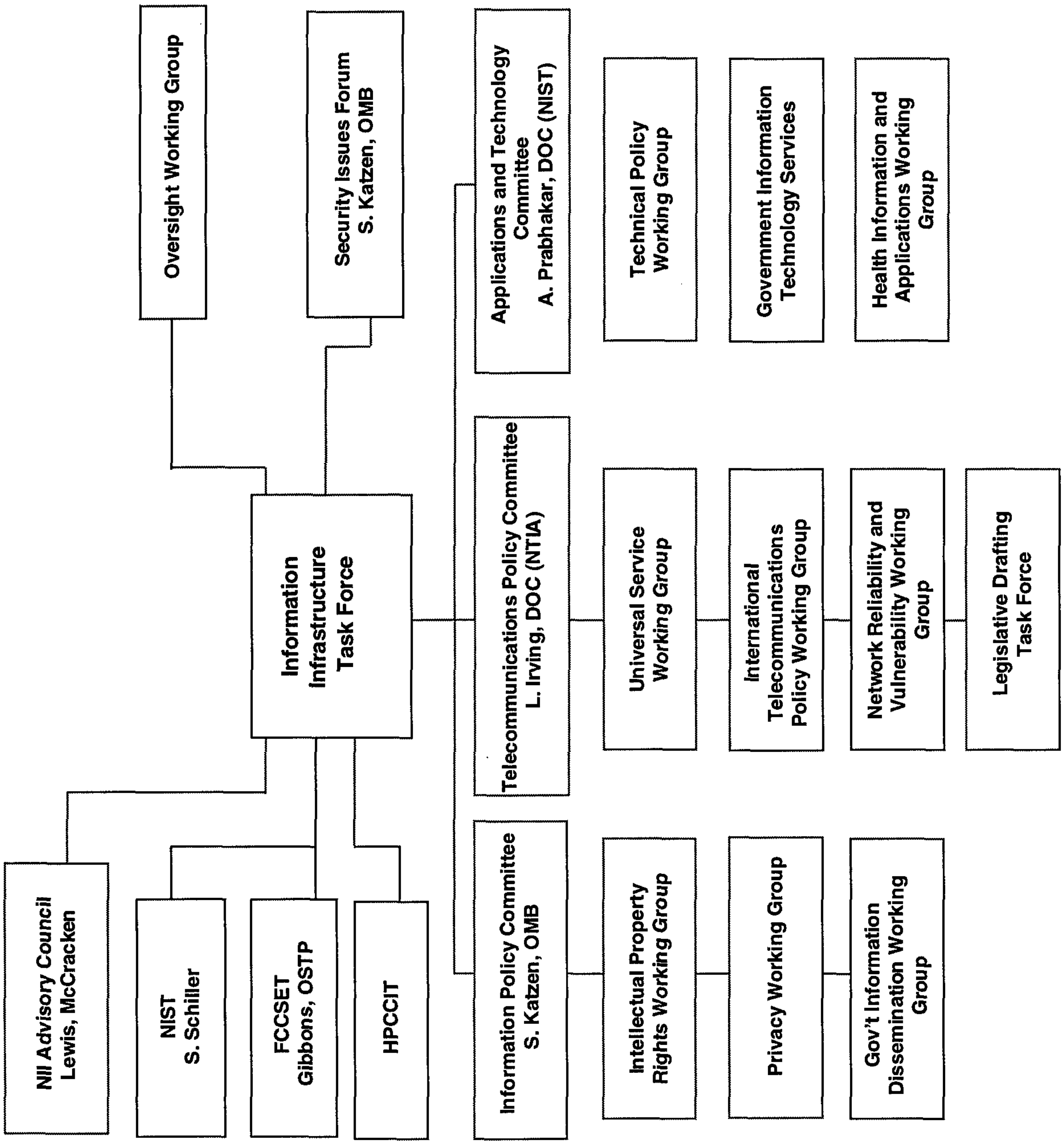
Agency for International Development
Commodity Futures Trading Commission
Department of Agriculture
  Federal Crop Insurance Corporation
Department of Agriculture
  Agricultural Marketing Service
Department of Commerce
  Patent and Trademark Office
Department of Commerce
  National Oceanographic and Atmospheric Administration
Department of Commerce
  Bureau of the Census
Department of Education

- Department of Energy
  - Federal Energy Regulatory Commission
- Department of Health & Human Services
  - Public Health Service
  - Health Care Financing Administration
  - Administration for Children & Families
- Department of Housing & Urban Development
- Department of Interior
  - Bureau of Land Management
- Department of Justice
  - Federal Bureau of Investigation
  - Immigration and Naturalization Service
- Department of Labor
  - Employment & Training Administration
  - Office of the Solicitor
  - Employment Standards Administration
  - Occupational Safety & Health Administration
  - Office of Administrative Law Judges
  - Bureau of Labor Statistics
  - Pension & Welfare Benefits Administration
  - Veterans Employment & Training Service
- Department of State
  - Bureau of Diplomatic Security
- Department of Transportation
  - Federal Railroad Administration
  - Maritime Administration
  - Federal Transit Administration
  - Research & Special Programs Administration
  - Federal Highway Administration
  - U.S. Coast Guard
  - National Highway Traffic Safety Administration
  - Federal Aviation Administration
- Department of Treasury
- Department of Veterans Affairs
  - IRM, Plan., Acq. & Security Service
- Environmental Protection Agency
- Equal Employment Opportunity Commission
- Executive Office of the President
- Farm Credit Administration
- Federal Communications Commission
- Federal Deposit Insurance Corporation
- Federal Emergency Management Agency
- Federal Maritime Commission
- General Accounting Office

General Services Administration
House of Representatives
    House Information Systems
Library of Congress
National Aeronautics & Space Administration
National Institute of Standards and Technology
National Labor Relations Board
National Science Foundation
National Security Agency
Nuclear Regulatory Commission
Office of Management and Budget
Office of Personnel Management
Resolution Trust Corporation
Securities and Exchange Commission
Small Business Administration
Social Security Administration
U.S. Information Agency
U.S. Senate
    Data Security Administrator
U.S. Supreme Court

Information Assurance Activities, Issues, Best Practices, Lessons Learned:

- The Forum is primarily an information sharing group, but has established some working groups on best practices and system access rules.
- The Forum holds an annual off-site meeting to concentrate on current security issues.


Oversight Working Group
Security Issues Forum
S. Katzen, OMB
Information
Infrastructure
Task Force
NII Advisory Council
Lewis, McCracken
NIST
S. Schiller
FCCSET
Gibbons, OSTP
HPCCIT
Applications and Technology
Committee
A. Prabhakar, DOC (NIST)
Technical Policy
Working Group
Government Information
Technology Services
Health Information and
Applications Working
Group
Telecommunications Policy Committee
L. Irving, DOC (NTIA)
Universal Service
Working Group
International
Telecommunications
Policy Working Group
Network Reliability and
Vulnerability Working
Group
Legislative Drafting
Task Force
Information Policy Committee
S. Katzen, OMB
Intellectual Property
Rights Working Group
Privacy Working Group
Gov't Information
Dissemination Working
Group

Organization: Information Infrastructure Task Force

Senior Information Assurance Official:

Secretary of Commerce

Information Assurance Points of Contact:

Information Policy Committee: Bruce McConnell
Intellectual Property Rights WG: Edward Kazenske
Privacy Working Group: Jerry Gates
Government Information WG: Peter Weiss

Telecom. Policy Committee: Tatia Williams
Universal Service Working Gp: Tatia Williams
Rel. and Vul. Working Gp: James Fletcher
Int. Telecom. Working Gp: Sharon Bywater
Legislative Drafting TF: Ellen Bloom

Committee on Appl's and Tech.: Cita Furlani
Gov't Info. Tech. Svcs (GITS): Jim Flyzik
Tech. Policy WG: Howard Frank
Health Info. and Appl's WG: John Silva

NII Security Issues Forum: Glenn Schlarman

Access to IITF Bulletin Board: 202/501-1920
IITF Secretariat: Susannah Schiller
IITF Committee Report: Susannah Schiller

On-Line Resources:

IITF Homepage: http://iitf.doc.gov/

Information Assurance Related Organizations, Missions and Functions:

The Clinton Administration formed the Information Infrastructure Task Force (IITF) to articulate and implement the Administration's vision for the National Information Infrastructure (NII). The task force consists of high-level representatives of the Federal agencies that play a major role in the development and application of information and telecommunications technologies.

Working together with the private sector, the participating agencies will develop comprehensive technology, telecommunications, and information policies and promote applications that best meet the needs of both the agencies and the country. By helping build consensus on difficult policy issues, the IITF will enable agencies to make and implement policy more quickly and effectively.

There are three IITF Committees: Information Policy Committee, Telecommunications Policy Committee, and a Committee on Applications and Technology.

Information Assurance Activities, Issues, Best Practices, Lessons Learned:

- A number of the IITF's subordinate efforts have, or will soon be, concluded. It is expected that a new smaller structure for the IITF will be proposed. The major areas of emphasis for continuing IITF activities will be health care, privacy, emergency management and public safety, security, and support of GII initiatives.

Organization: Security Issues Forum, IITF

Senior Information Assurance Official:

Salley Katzen, Chairperson, SIF

Information Assurance Points of Contact:

Glenn Schlarman

Information Assurance Related Missions and Functions:

The NII Security Issues Forum will provide leadership for Federal NII security activities. It will ascertain the security needs of the various NII user communities and the Federal role in assuring such security. It will ensure coordination of the security activities across the various Committees of the IITF and serve as a clearinghouse for Federal security efforts related to the NII. The Forum will also consider the scope of legal and policy remedies necessary to achieve desired security in the NII.

The Forum coordinates the following IITF activities:

- Telecommunications Policy Committee (TPC), the Information Policy Committee (IPC), and the Committee on Applications and Technology (CAT).
- Intellectual Property Rights Working Group (IPRWG) and the Privacy Working Group (PWG).
- The Government Information Technology Services Working Group (GITS), will advise the Forum on security issues pertaining to the application of information technology by Federal agencies to improve service delivery and accomplish agency missions.

The Forum also coordinates the efforts of the following Federal government entities:

- National Institute of Standards and Technology (NIST) will encourage the Computer System Security and Privacy Advisory Board (CSSPAB).
  NIST, will assess where research and development on security technology would be useful for the NII.
- NIST, working with other agencies, will identify Federal security products, techniques, and practices that will be useful in the NII.
- NIST will work with the Forum of Incident Response and Security Teams (FIRST) to assess how private entities conduct emergency response and how the efforts of Government can be coordinated with them to ensure a "911" capability for the NII.
- National Communications System (NCS), in coordination with the industry's National Security Telecommunications Advisory Committee (NSTAC), will work with the Reliability and Vulnerability Working Group to ensure that National

Security and Emergency Preparedness (NS/EP) needs are accommodated in the NII.

- National Security Telecommunications and Information Systems Security Committee (NSTISSC) will identify useful security tools and techniques in the national security community that may be applicable to the NII.
- Working Group on Encryption and Telecommunications (WGET) will develop policy recommendations regarding the Government's response to the spread of digital telecommunications equipment and inexpensive encryption devices which could prevent effective wiretaps.
- The High Performance Computing and Communications (HPCC) Program will assure development and testing of new technologies for computer security suitable to a high performance environment.
- The Federal Network Council (FNC), a multi-agency committee that oversees Federal research networks, shall explore specific issues relating to security of the Internet.

Information Assurance Activities, Issues, Best Practices, Lessons Learned:

- SIF has published a draft report, "NII Security: The Federal Role." The plan will be based on the series of public meetings on NII security held by the SIF. The plan will be subjected to public discussion. It will address security concerns, how to meet the concerns (market forces, private investment, government investment, etc.), legislative proposals, and a possible need for a Federal government response and recovery plan.
- At a March 1996 meeting, the forum decided to focus it efforts on the following three issues:
  - Cryptography policy
  - Infrastructure Assurance
  - Assess the need for assurance for security products and who should do it.
- Regulatory oversight provides an opportunity to influence security in the infrastructures. While government regulatory activity is being reduced, regulation of information technology and security practices might have to increase.

Organization: Reliability and Vulnerability Working Group, IITF

Senior Information Assurance Official:

Information Assurance Points of Contact:

James Fletcher

Information Assurance Related Missions and Functions:

The RVWG has established four subgroups:

Reliability for General Users: This group is addressing issues related to overall NII reliability for Government, industry, and general users in the context of both day-to-day and emergency operations. It has identified strategies for ensuring reliability.

National Security and Emergency Preparedness: This group is addressing issues related to the NS/EP attributes the NII should support. This effort includes reviewing key industry segments such as the public switched network, cable, wireless, satellite, and broadcast and identifying features and capabilities that should be available over the NII to support NS/EP users.

Protection of the Network: This group is addressing issues related to protecting key network elements from unauthorized intrusion or manipulation and is seeking to ensure that network management information is protected. It is developing a report that will describe the potential challenges to protecting the network in the evolving NII, the threats to and vulnerabilities of the network, the resulting risks to the NII, and current efforts to reduce risks. It will conclude with an approach for addressing the system protection problem in the NII.

Integration and Planning: This group has taken inputs from each of the other subgroups and melded them into a proposed action plan that addresses reliability and vulnerability concerns. The plan describes problems, as well as key issues and necessary actions, in the areas of policy, legislation, management mechanisms, and technology. The subgroup will accomplish its objective by using an integrating framework that is currently in draft and is being addressed by the RVWG.

Information Assurance Activities, Issues, Best Practices, Lessons Learned:

- The RVWG has issued a report entitled *"NII Risk Assessment: A Nation's Information at Risk."* The report concluded that:
  - There are real and active threats to the NII and those threats will grow over time.
  - There is not enough information available to conduct a more rigorous analysis of the NII.
  - There is no common framework, approach, or terminology for discussing or analyzing risks to the NII.
  - No sound mechanism exists for government and industry to share information necessary for future sound risk assessments on individual systems.
  - Risk management must be a coordinated effort involving many different activities.
  - Because the NII is so broad and complex, its risk can only be assessed at a high level.
- The emphasis of the reports recommendations were centered on the need to establish mechanisms to support information exchange between all NII users detailing how they use the NII, how the risks to the NII will affect them, and what to do to manage those risks.
- The RVWG has formally declared the conclusion of its activities and is expected to disband within the next year.
- The RVWG has also established a working relationship with the President's National Security Telecommunications Advisory committee (NSTAC) through its NII Task Force. The RVWG subgroup leaders met with the Chairs of the NII Task Force and its three subgroup chairs to discuss issues of mutual interest and to determine how to make their efforts complementary. RVWG representatives, including the subgroup leaders, have attended meetings of the NII Task Force to continue the dialogue between the two organizations. In particular, the RVWG NS/EP subgroup has met with the NSTAC NII Task Force Architecture Subgroup and factored industry's input into its efforts to identify NII NS/EP features and capabilities.
- The RVWG determined that its overall objective was to ensure that telecommunications services and information systems of the national information infrastructure will provide: high quality service for normal operations; maximum reliability of services to meet essential public, private, and commercial needs; and capabilities that meet national security and emergency preparedness requirements. The working group agreed that the best approach to achieve that objective would be to focus on top level actions that address its span of responsibilities. The proposed Plan of Action identifies top level actions that will be pursued by the RVWG, in partnership with industry and government user groups. The plan recommends tasking for specific government agencies, recommends tasking to and from other IITF committees and working groups, and develops strategies to leverage industry and other user groups to accomplish these actions.
- The Group is developing a Reliability and Vulnerability Working Group Work Plan. The RVWG subgroups have been reviewing the proposed actions and identifying milestones to accomplish those actions. For each milestone, they are setting target dates and proposing candidate offices of primary responsibility. The RVWG plans to reach consensus on its Plan of Action. It is expected that the Plan of Action will be a "living document," capable of responding to the dynamic NII environment.

Organization: Information Management Policy Working Group

Senior Information Warfare Official:

Information Warfare Points of Contact:

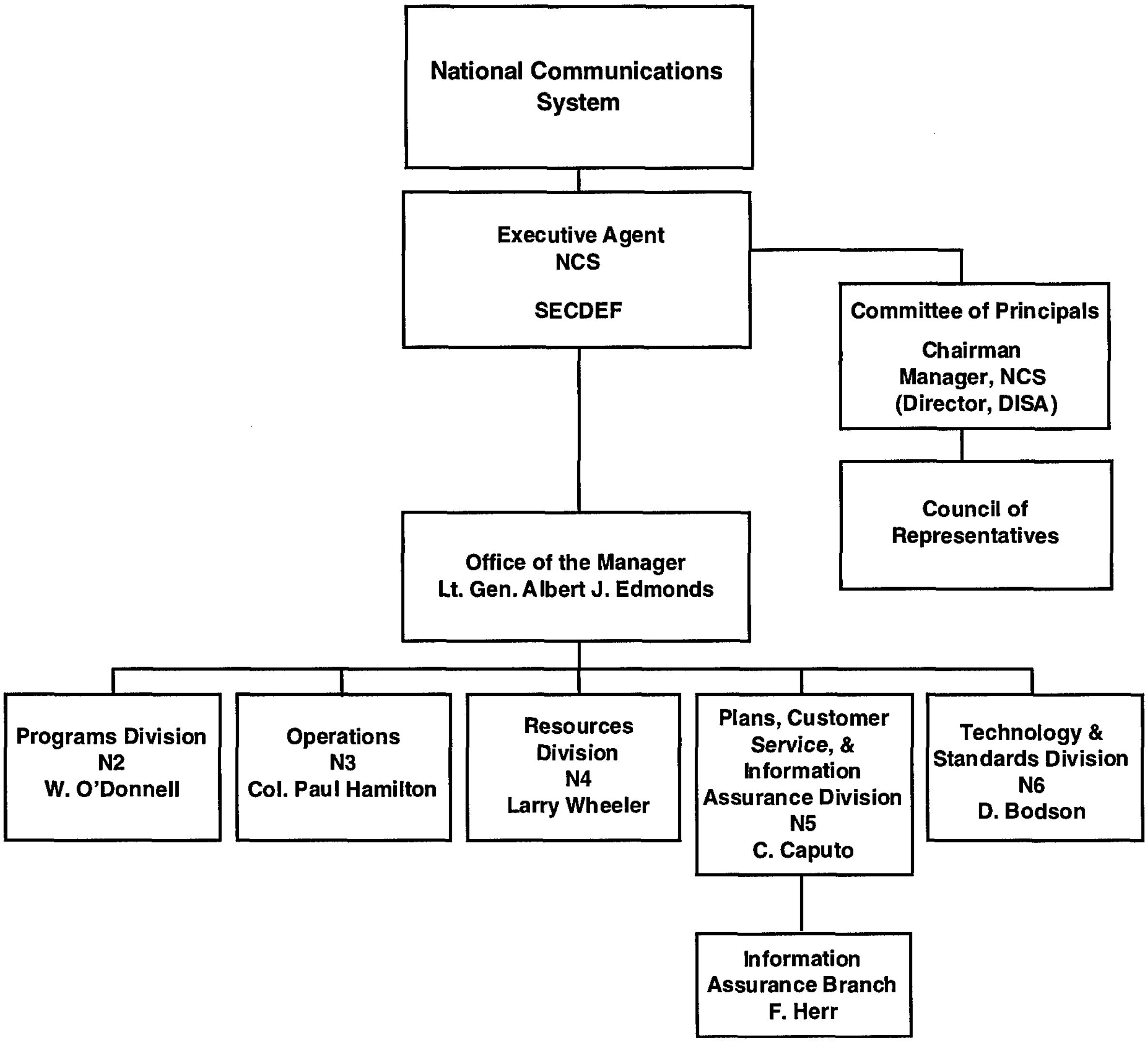
On-Line Resources:

Information Warfare Related Missions and Functions:

The IMPWG is a joint DoD/DCI group created to support the Information Systems Board (ISB). Chaired by the Executive Director for Intelligence Community Affairs and the Deputy Assistant Security of Defense (Intelligence and Security), the ISB advises the DCI and the Deputy Secretary of Defense on information security matters as they pertain to interaction among organizations under their purview. The IMPWG, in turn, establishes automated intelligence information systems management and associated security policy and programs. The mission of IMPWG is to recommend top-level architectures; adopt community standards; develop policy to effect connectivity and common-user infrastructure, and interoperability; provide program and budget support; and provide liaison and coordination on security and technology issues.

Membership consists of DIA, CIA, NSA, CIO, Joint Staff, NRO, Military Services, DMA, DISA, State, Treasury, DoE, FBI, Commerce, and additional organizations as necessary. Accomplishments of the IMPWG include devising and issuing a security risk assessment methodology.

Information Warfare Activities, Issues, Best Practices, Lessons Learned:


National Communications System
Executive Agent NCS SECDEF
Committee of Principals Chairman Manager, NCS (Director, DISA)
Council of Representatives
Office of the Manager Lt. Gen. Albert J. Edmonds
Programs Division N2 W. O'Donnell
Operations N3 Col. Paul Hamilton
Resources Division N4 Larry Wheeler
Plans, Customer Service, & Information Assurance Division N5 C. Caputo
Technology & Standards Division N6 D. Bodson
Information Assurance Branch F. Herr

Organization: National Communications System (NCS)

Senior Information Assurance Official:

Lieutenant General Al Edmonds, Manager, NCS

Information Assurance Points of Contact:

Fred Herr, Office of the Manager, NCS

On-Line Resources:

NCS Homepage: http://164.117.147.223/

Information Assurance Related Missions and Functions:

The Interdepartmental Committee on Communications was formed by the National Security Council on October 26, 1962, to resolve the major communications problems which had surfaced during the Cuban missile crisis. The Committee's work resulted in the creation of the NCS on August 21, 1963. The NCS was updated by Executive Order 12472, April 3, 1984, and is charged with assisting the President, the National Security Council, the Office of Science and Technology Policy, and the Office of Management and Budget in the exercise of their wartime and non-wartime emergency telecommunications functions, and their planning and oversight responsibilities. The NCS also assists in the coordination of planning for and the provision of national security and emergency preparedness telecommunications of the Federal government under all circumstances, including crisis or emergency, attack, recovery, and reconstitution. In addition, the Office of the Manager, NCS (OMNCS), provides administrative support to the President's National Security Telecommunications Advisory Committee.

Membership includes:

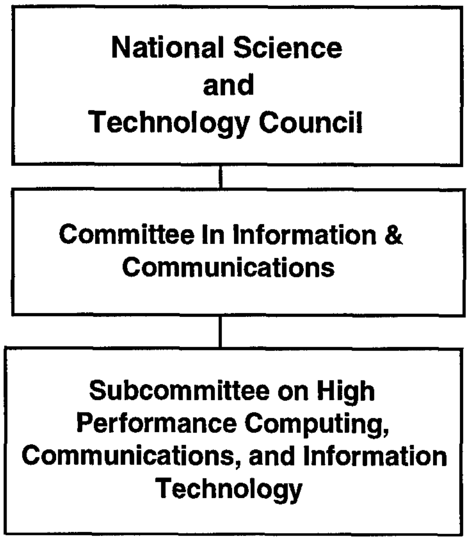
Department of Agriculture
Department of Commerce
Department of Defense
Department of Energy
Department of Health and Human Services
Department of Justice
Department of State
Department of the Interior
Department of the Treasury
Department of Transportation
Department of Veterans Affairs
Central Intelligence Agency
Federal Communications Commission

Federal Emergency Management Agency
Federal Reserve System
General Services Administration
The Joint Staff
National Aeronautics and Space Administration
National Security Agency
National Telecommunications and Information Administration
Nuclear Regulatory Commission
United States Information Agency
United States Postal Service

Information Assurance Activities, Issues, Best Practices, Lessons Learned:

- GETS. The Government Emergency Telecommunications Service provides National Security/Emergency Preparedness (NS/EP) users with dependable and flexible switched voice and voice-band data communications during times of extreme emergency or war. GETS derives its service from the assets and capabilities of the Public Switched Network (PSN). This emergency telecommunications service is provided by a variety of techniques. One technique is to restrict access to the priority services to only NS/EP users. Another technique is to provide priority treatment for GETS calls in the form of priority trunk queuing and reservation, exemption from restrictive management controls (e.g., call blocking) imposed during periods of excessive network loading, and the use of a special NS/EP identifier for priority call identification and call set up. Finally, routing of the NS/EP calls through the network is accomplished by an enhanced process which increases the number of possible routes searched -- in normal operations, a trunk busy signal is returned to the originator of the call in the event the signaling system makes three unsuccessful attempts to find a route to the call destination.
- The current GETS requirements and operational concept are based on six functional requirements for NS/EP telecommunications that were defined in an Executive Office of the President Memorandum (dated October 15, 1991) on the National Level Telecommunications Program Implementation and Functional Requirements.
- The Government Emergency Telecommunications Service (GETS) achieved its initial operating capability on 1 October 1995.
- High Probability of Completion (HPC) is an American National Standards Institute (ANSI) SS7 network capability standard (ANSI T1.631-1993) for identification of NS/EP calls in SS7 networks creating a means for identifying GETS traffic within the Public Switched Network (PSN) on a call-by-call basis and triggering the activation of priority treatment and other enhancements.
- The NCS managed Telecommunications Service Priority System (TSP) establishes the regulatory, administrative, and operational framework to authorize the priority provisioning and restoration of NS/EP telecommunications services. This allows vendors to initiate, restore, or otherwise act on a priority basis to ensure effective NS/EP telecommunications.

- The Director, NSA, briefed the National Security Telecommunications Advisory Committee (NSTAC) in January 1995 on the threat really pushing NSTAC/NCS model for other industries. Director FBI also spoke to NSTAC after recent Executive Session. IES members met with CAPT Dave Henry and Mr. Dave Patterson of NSA to discuss threat. Jack Edwards briefed NSTAC response to McConnell briefing at last NSTAC meeting.
- Have briefed J33 and J6 on on-going efforts. Also briefed personnel from the Office of the Secretary of Defense (OSD) Net Assessment and Office of the Under Secretary of Defense Policy (USD(P)).
- National Defense Infrastructures Survivability Study by USD(P) is underway. Being done by DNA as a successor to the Key Asset Protection Program (KAPP).
- NII Symposium conducted at NWC in Newport last October.
- Bellcore has 5-year contract with OMNCS to collect Public Switched Network (PSN) vulnerability and incident data. The data collected will build on Bellcore's Security Information Exchange data.
- SRI has produced hacker profile for OMNCS.
- The February 1996 NSTAC focused on IA with briefings by Deputy Attorney General, Jamie Goulick; Secretary Policy Board Staff Director, Peter Soderholm; Center for Strategic & International Studies; Director, Arnaud De Borchgrave; and Jeffrey Symoth, General Counsel, CIA. Senator Jon Kyl, author of the Kyl Amendment to the Defense Authorization Bill spoke to NSTAC during the Executive Breakfast.


National Science and Technology Council
Committee In Information & Communications
Subcommittee on High Performance Computing, Communications, and Information Technology

Organization: National Science and Technology Council

Senior Information Assurance Official:

Information Assurance Points of Contact:

On-Line Resources:

NSTC Homepage:
http://www.whitehouse.gov/WH/EOP/OSTP/NSTC/html/NSTC_Home.html

Information Assurance Related Missions and Functions:

President Clinton established the National Science and Technology Council (NSTC) by Executive Order 12881 on November 23, 1993. This cabinet-level council is the principal means for the President to coordinate science, space, and technology policies across the Federal government.

An important objective of the NSTC is the establishment of clear national goals for Federal science and technology investments in areas ranging from information technologies and health research, to improving transportation systems and strengthening fundamental research. The Council prepares research and development strategies that are coordinated across Federal agencies to form an investment package that is aimed at accomplishing multiple national goals.

<u>Membership</u>:
The President
The Vice President
Secretary of State
Secretary of Defense
Secretary of Interior
Secretary of Agriculture
Secretary of Commerce
Secretary of Labor
Secretary of Health and Human Services
Secretary of Transportation
Secretary of Energy
Secretary of Education
Director, Office of Management and Budget
Assistant to the President for Science and Technology
Assistant to the President for National Security Affairs
Assistant to the President for Economic Policy

Assistant to the President for Domestic Policy
Chair of the Council of Economic Advisors
Administrator, National Aeronautics and Space Administration
Administrator, Environmental Protection Agency
Director, National Science Foundation
Director, National Institutes of Health
Director, Central Intelligence Agency
Director, Arms Control and Disarmament Agency

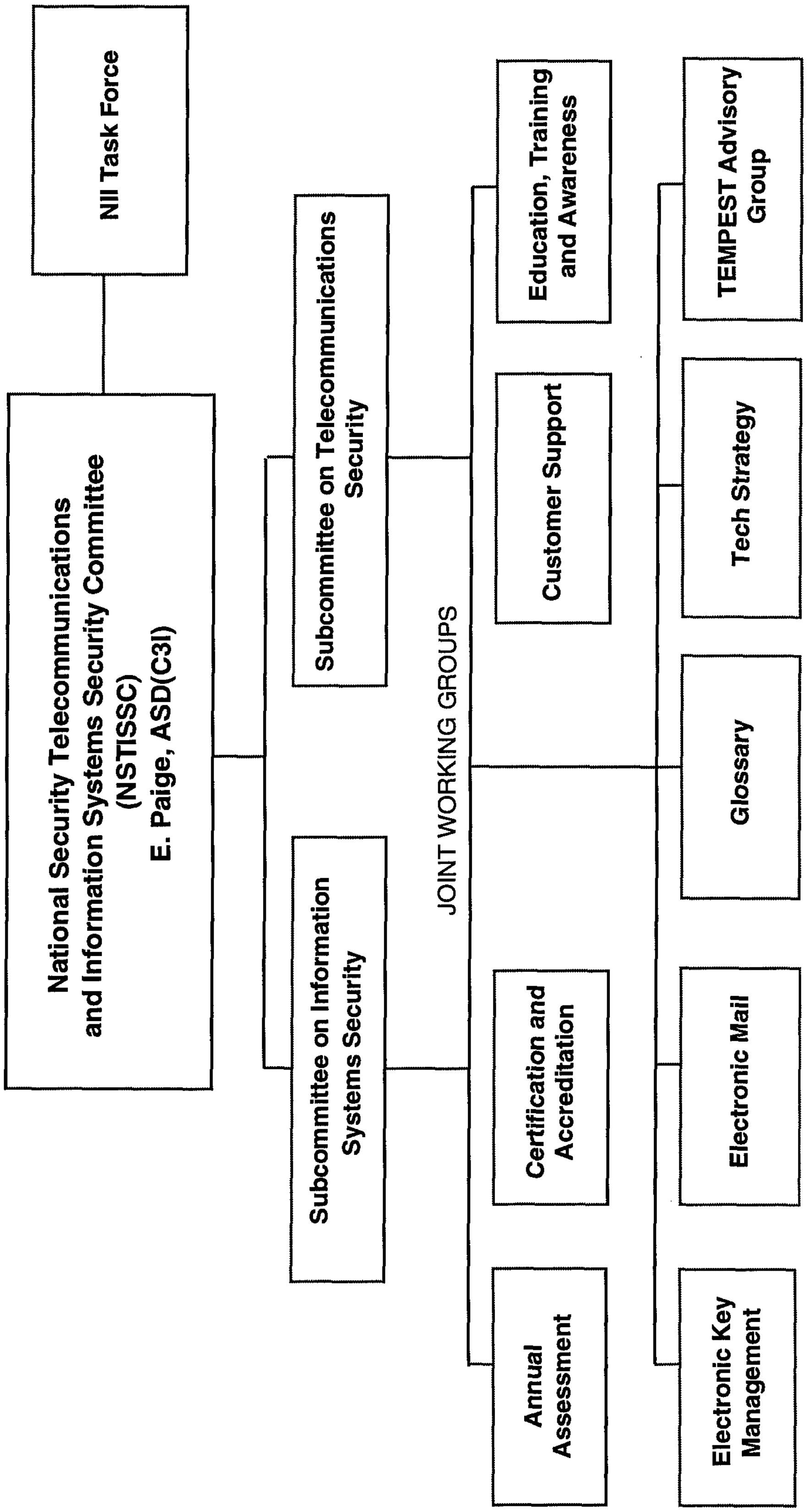
President Clinton directed the NSTC to:

- Coordinate the science and technology policy making and implementation process across Federal agencies;
- Ensure that science and technology policy decisions are consistent with the President's stated goals;
- Ensure that science and technology issues are considered in the development and implementation of Federal policies and programs;
- Further international cooperation in science and technology activities.

The Council fosters a strategic approach in determining how science and technology can help resolve complex societal needs. Today's problems demand contributions from different fields of study and a team approach from the agencies that make up the Federal R&D enterprise. The NSTC provides an interagency strategic management system to foster teamwork and enhance the ability to identify opportunities for interdisciplinary solutions.

Information Assurance Activities, Issues, Best Practices, Lessons Learned:

This page intentionally left blank.


NII Task Force
National Security Telecommunications and Information Systems Security Committee (NSTISSC) E. Paige, ASD(C3I)
Subcommittee on Telecommunications Security
Subcommittee on Information Systems Security
JOINT WORKING GROUPS
Education, Training and Awareness
Customer Support
Certification and Accreditation
Annual Assessment
TEMPEST Advisory Group
Tech Strategy
Glossary
Electronic Mail
Electronic Key Management

Organization: National Security Telecommunications and Information Systems Security Committee (NSTISSC)

Senior Information Assurance Official:

E. Paige, Assistant Secretary of Defense (C3I), Chairman

Information Assurance Points of Contact:

NSTISSC Secretariat (Located at NSA)

On-Line Resources:

Information Assurance Related Missions and Functions:

NSTISSC was created via NSD 42, dated 5 July 1990. NSD 42 established a senior level policy coordinating committee under the NSC, an interagency group at the operating level (NSTISSC), two subcommittees (one for information systems security and one for telecommunications security), an executive agent (DoD), and a national manager (NSA). The Policy Coordinating Committee provide a "tie breaking" decision when issues cannot be resolved at the NSTISSC level. The Policy Coordinating Committee has been required to meet on only one occasion in the NSTISSC's history. The NSTISSC's mission is to consider technical matters and develop operating policies, guidelines, instructions, and directives, as necessary to implement the provisions of the Directive. Specific matters are addressed by joint working groups as required.

The NSTISSC's National Information Infrastructure (NII) Executive Committee and the NII Task Force (NIITF) were established to develop and implement a comprehensive and proactive program in support of the NII. The Executive Committee provides guidance and direction to the NIITF, oversees its activities, maintains liaison with NIST, as appropriate, and reports periodically to the NSTISSC on its progress. The NIITF is comprised of individuals representing NSTISSC member and observer organizations and is responsible for all NSTISSC support to the NII including:

- Facilitating liaison with various NII fora
- Coordinating the activities of NSTISSC Sub working groups in support of the NII
- Developing white papers on security issues of concern to the NII
- Providing an analysis of the common security services and requirements of member organizations
- Publishing an annual compendium of government information safeguard requirements
- Developing and implementing a campaign to increase awareness of security issues.

NSTISSC membership is categorized as follows:

- Member on the NSTISSC, STS, and SISS
- Observer on the NSTISSC, STS, and SISS
- Observer on the STS and SISS
- Observer on the STS
- Observer on the SISS
- Working Group Member

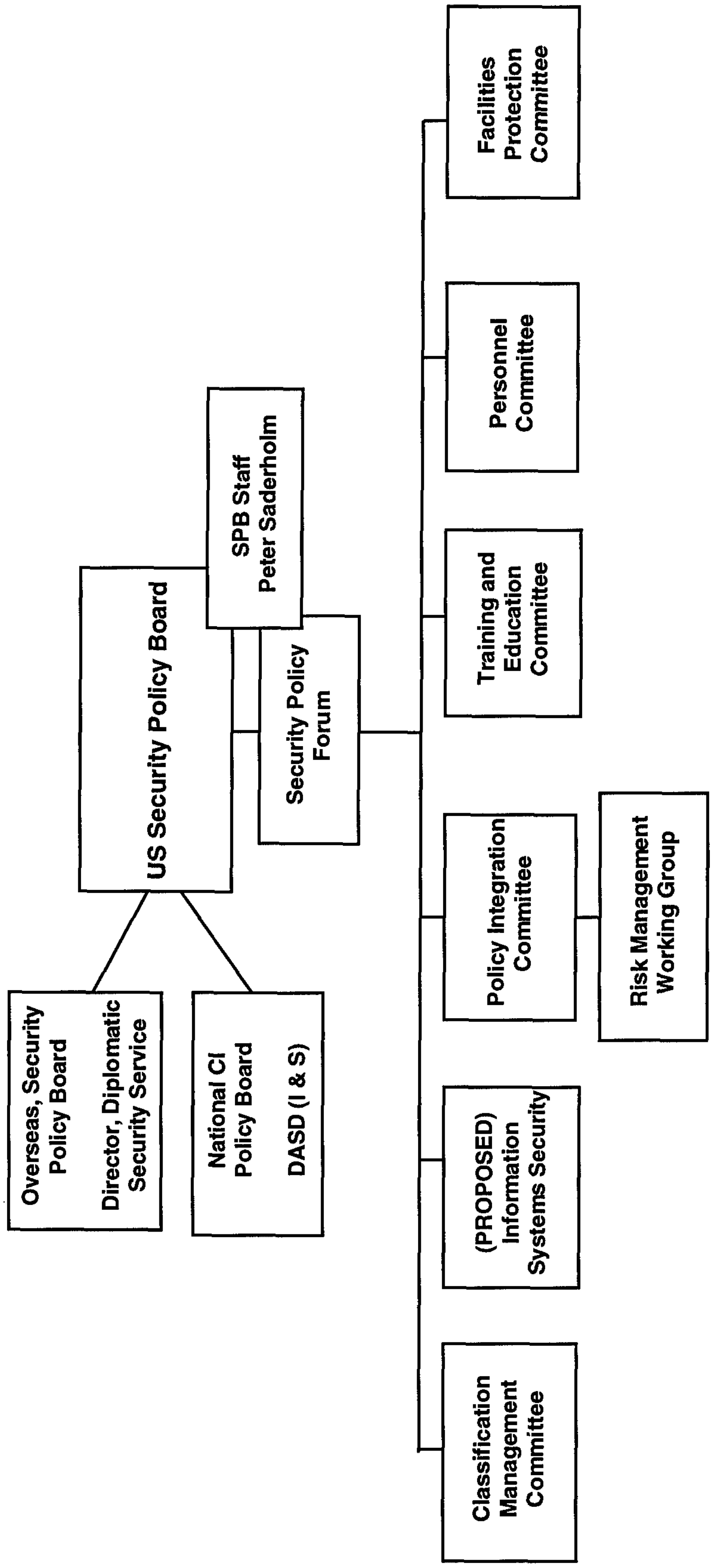
Membership in the various categories includes the following organizations. Details of which members belong to which categories can be obtained from the NSTISSC Secretariat. Where both a parent and subordinate organization are shown, both organizations participate in one or more of the above categories.

National Security Council Staff
Office of Management and Budget
U.S. Department of Agriculture
Department of Commerce
National Institute of Standards and Technology
Department of Defense
Joint Staff
Army
Navy
Marine Corps
Air Force
Defense Information Systems Agency
White House Communications Agency
Defense Intelligence Agency
Defense Investigative Service
Defense Logistics Agency
Defense Mapping Agency
Defense Nuclear Agency
National Security Agency
Department of Education
Department of Energy
Department of Health and Human Services
Indian Health Service
Public Health Service
Department of Housing and Urban Development
Department of the Interior
Department of Justice
Drug Enforcement Administration
Federal Bureau of Investigation
Immigration and Naturalization Service
Department of Labor

Department of State
Department of Transportation
Federal Aviation Administration
U.S. Coast Guard
Department of the Treasury
U.S. Customs Service
U.S. Secret Service
Department of Veterans Affairs
Director of Central Intelligence/Central Intelligence Agency
Federal Communications Commission
Federal Emergency Management Agency
Federal Reserve System
General Services Administration
National Aeronautics and Space Administration
National Communications System
Nuclear Regulatory Commission
Office of Personnel Management
Securities Exchange Commission
U.S. Information Agency

Information Assurance Activities, Issues, Best Practices, Lessons Learned:

- NSTISSC accomplishments to date include the development of policies, guidelines, instructions, and standards; provided systems security guidance; produced the annual assessment of the "health" of national security systems; provides release approvals to foreign governments and international organizations; maintained the national issuance system; and produced special publications.


US Security Policy Board
SPB Staff
Peter Saderholm
Security Policy
Forum
Overseas, Security
Policy Board
Director, Diplomatic
Security Service
National CI
Policy Board
DASD (I & S)
Classification
Management
Committee
(PROPOSED)
Information
Systems Security
Policy Integration
Committee
Risk Management
Working Group
Training and
Education
Committee
Personnel
Committee
Facilities
Protection
Committee

Organization: United States Security Policy Board (USSPB)

Senior Information Assurance Official:

Peter Saderholm, Director, USSPB Staff

Information Assurance Points of Contact:

Vicki LaBarre, USSPB Staff
Dan Knauf, USSPB Staff

On-Line Resources:

Information Assurance Related Missions and Functions:

The Secretary of Defense (SECDEF) and the Director of Central Intelligence (DCI) created the Joint Security Commission (Commission) in May 1993 to review the security practices and procedures under their authorities.

The Commission concluded that the problems of fragmentation and inconsistency in security policy development, implementation, and oversight must be resolved in order to make meaningful improvements in the overall effectiveness of US Government security. The commission proposed the creation of a unifying structure to "provide leadership, focus, and direction to the government security communities."

Under PDD-29, the U.S. Security Policy Board became the umbrella under which all the elements of security are organized. It is responsible for not only what to protect (classification management) but also how to protect it (security countermeasures). The Board receives overall policy guidance from the NSC and accepts responsibility for the flow of policy direction both to and from the NSC. Consistent with PDD-29, the Board is assisted by the Security Policy Advisory Board (Advisory Board), the Security Policy Forum (Forum), and various intergovernmental committees and working groups.

Committees and ad hoc working groups organized along security discipline lines support the Forum. The principle committees proposed to support the Board structure include:

- A Personal Security Committee (PSC) to address all personnel security policies, procedures, and practices applicable to US Government departments and agencies;

- A Facilities Protection Committee (FPC) to address all policies, practices and procedures applicable to the protection of US Government and industrial facilities; physical, technical, and TEMPEST;

- A Classification Management Committee (CMC) charged with the development of classification management policy within the context of the overall security policy framework;

- A Training and Professional Development Committee (TPDC) to standardize and coordinate security training, education, and awareness and to achieve efficiencies in the development and delivery of such training, and;

- A Policy Integration Committee (PIC) charged to ensure overarching themes are integrated into all U.S. Government security policy and encourage synergy in the activities of the other standing committees.

- An Information Systems Security Committee - TBD

As of 1 June 1995, all committees have been established except the Information Systems Security Committee. (See attachment.)

Information Assurance Activities, Issues, Best Practices, Lessons Learned:

- The end of the Cold War has dramatically changed the threats that defined the security policies and procedures for protecting our government's information, facilities and people. While some threats have been reduced, others have remained relatively stable or have increased. Our understanding of the range of issues that affect our national security continues to evolve. Economic issues are of increasing concern and are competing with traditional political and military issues for resources and attention. Technologies, such as those used to create weapons of mass destruction are evolving and proliferating. With this greater diversity of threats, there is wide recognition that the security policies, practices, and procedures developed during the Cold War must be reexamined and changed. We require a new security process based on sound threat analysis and risk management practices. A process which can adapt our security policies, practices and procedures as the economic, political and military challenges to our national interests continue to evolve.
- The Director of Central Intelligence and Secretary of Defense's Joint Security Commission identified four principles which should guide the formulation, evaluation and oversight of our security policy:
  - Our security policies and services must realistically match the threats we face and must be sufficiently flexible to facilitate change as the threats evolve.
  - Our security policies and practices must be consistent and enable us to allocate scarce resources effectively.
  - Our security standards and procedures must result in the fair and equitable treatment of all Americans upon whom we rely to guard our nation's security.
  - Our security policies, practices and procedures must provide the security we need at a price we can afford.
- The National Security Act of 1947, as amended, specifies that is the duty of the National Security Council (NSC) to consider policies on matters of common interest to the departments and agencies of the Government concerned with the national security and to

make recommendations to the president in connection therewith. Consistent with the National Security Act of 1947, the President directed the establishment of a new security policy structure, under the direction of the NSC, for the coordination, formulation, evaluation and oversight of security policy guided by the above principles.

- Nothing in this directive amends or changes the authorities and responsibilities of the members of the Policy Board, including, Director of Central Intelligence (DCI), Secretary of Defense, Secretary of State, Secretary of Energy, Secretary of Commerce, Attorney General, Director of the FBI, Chairman of the Nuclear Regulatory Commission, or Director of the Information Security Oversight Office as contained in the National Security Act of 1947, other existing laws or Executive Orders.
- The President directed the following:
    - The Joint Security Executive Committee established by the Deputy Secretary of Defense and the Director of Central Intelligence was designated the Security Policy Board and directed to report to the President through the Assistant to the President for National Security Affairs. The existing national security countermeasures policy and coordination structure, the National Advisory Group for Security Countermeasures, was thereby abolished and its functions transferred to the Security Policy Board.
    - The Security Policy Board consists of the Director of Central Intelligence, the Deputy Secretary of Defense, Vice Chairman of the Joint Chiefs of Staff, the Deputy Secretary of State, the Under Secretary of Energy, the Deputy Secretary of Commerce, the Deputy Attorney General, one Deputy Secretary from another non-defense related agency and one representative from the Office of Management and Budget and the NSC staff. The additional non-defense agency representative will be rotated on an annual basis and selected by the non-defense agency members of the Security Policy Forum established below. Senior representatives of other Departments and Agencies will be invited members at such times as the Security Policy Board considers security issues germane to their responsibilities.
    - The Chairman of the Security Policy Board was designated by the Assistant to the President for National Security Affairs on behalf of the President.
    - The Security Policy Board considers, coordinates and recommends for implementation to the President, through the Assistant to the President for National Security Affairs, policy directives for U.S. security policies, procedures and practices. The Security Policy Board is the principal mechanism for reviewing and proposing to the NSC legislative initiatives and executive orders pertaining to U.S. security policy, procedures and practices that do not fall under the statutory jurisdiction of the Secretary of State. This Board coordinates the development of interagency agreements and resolve conflicts that may arise over the terms and implementation of these agreements. In coordinating security policy, procedures and practices, the Policy Board ensures that all U.S. Departments and Agencies affected by such decisions are allowed to comment on such proposals.
    - Policy disputes that cannot be resolved by this Board are forwarded to the Principals Committee of the National Security Council.
    - A Security Policy Advisory board was established to serve as an independent and non-governmental advisory body on U.S. security policy. Five members, including

a Chairman, will be appointed by the President for terms of up to three years. As of June 1966, the Chairman and two members have been appointed and are being briefed in preparation for their first meeting. The Chairman will report annually to the President through the Assistant to the President for National Security Affairs on implementation of the four policy principles identified above. The Security Policy Advisory Board will also provide a non-governmental and public interest perspective on security policy initiatives to the Security Policy Board and the intelligence community.

- The Security Policy Forum established under the Joint Security Executive Committee was retained under the Security Policy board to consider security policy issues raised by its members or any other means; develop security policy initiatives and obtain Department and Agency comments on these initiatives for the Policy Board; evaluate the effectiveness of security policies; monitor and guide the implementation of security policy to ensure coherence and consistency; and oversee the application of security policies to ensure that they are equitable and consistent with national goals. Policy Forum membership includes one senior representative from the Office of Secretary of Defense, Joint Chiefs of Staff, each Military Department, including the U.S. Coast Guard, Defense Intelligence Agency, National Security Agency, Central Intelligence Agency, Commerce, Energy, Justice, State, Treasury, Transportation, Federal Bureau of Investigation, National Reconnaissance Office, Federal Emergency Management Agency, General Services Administration, Defense Information Systems Agency/National Communications System, Office of personnel Management, Information Security Oversight Office, Nuclear Regulatory Commission, NASA, Office of Management and Budget, Department of Interior, National Archives, Department of Agriculture, and other agencies representatives as invited by the Security Policy Board Chairman.
- The Security Policy Board and Forum has established interagency working groups as necessary to carry out their functions and ensure interagency input and coordination of security policy, procedures and practices. When the work of the group is concluded, the group is dissolved.
- The existing Department of State Overseas Security Policy Group is hereby designated as, and its functions transferred to, the Overseas Security Policy Board and directed to report to the president through the Assistant to the President for National Security Affairs. The Overseas Security Policy Board is chaired by the Director of the Diplomatic Security Service and its membership consists of representatives from the Department of State, Agency for International Development, CIA, Defense Intelligence Agency, FBI, Commerce, Justice, Treasury, Transportation, National Security Agency, United States Information Agency, Peace Corps, Federal Aviation Administration, Foreign Agricultural Service and the DCI's Center for Security Evaluation, Office of Management and Budget, NASA, Arms Control and Disarmament Agency.
- The Overseas Security Policy Board considers, develops, coordinates and promotes policies, standards and agreements on overseas security operations,

programs and projects which affect all U.S. Government agencies under the authority of a chief of mission abroad.

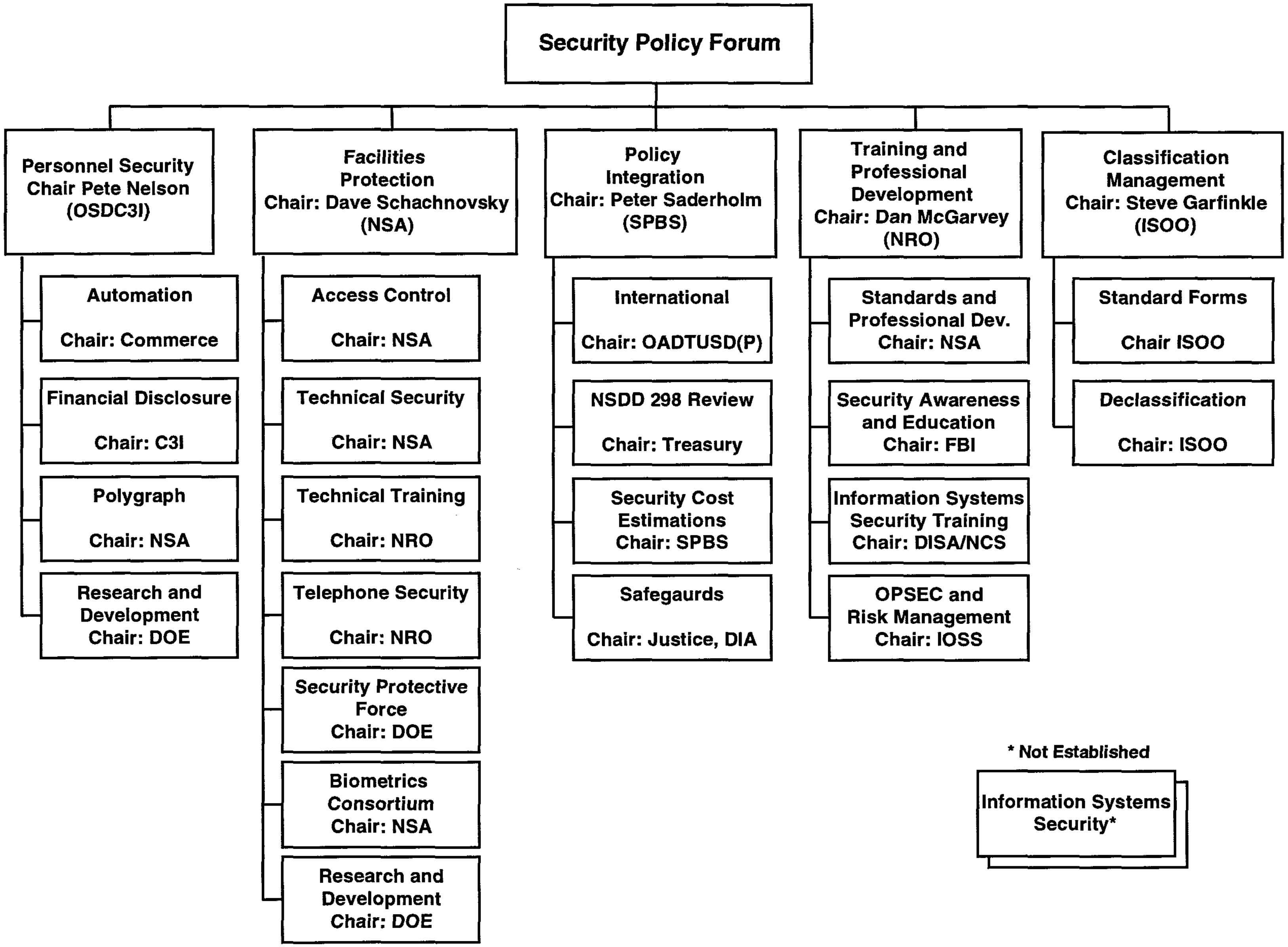
- The National Counterintelligence Policy Board established by PDD-24, the Security Policy Board, and the Overseas Security Policy Board, will coordinate as necessary on policy issues that may be of mutual concern, and each Board will implement procedures for such coordination. Conflicts between these Boards that cannot be resolved will be referred to the Principals Committee of the National Security Council. The Chairman of these Boards will meet at least on an annual basis to review policy coordination.
- The Security Policy Board, Forum, and any interagency working groups established by these bodies will be supported by a Staff which will operate under the direction of the Security Policy Board. This Staff will also provide administrative and personnel support to the Security Policy Advisory Board, which will operate independent of other Staff functions and personnel under the direction of the Chairman of this Advisory Board. Staff personnel will be provided or funded by the member agencies of the Security Policy Board.

- During its first year, the Board, with its substructure of the Security Policy Forum (Forum), five standing committees, and ad hoc working groups, all regularly kept informed by key industrial representatives, has served to facilitate reciprocity and commonality by engaging 27 federal agencies and departments in the dialogue and process that lead to national policy formulation. The Board, composed of 10 deputy secretaries or under secretaries or equivalent, functions primarily to rule on policies formulated by the Forum and standing committees and, when required, resolve conflicts that arise the substructures, Such a high-level conflict resolution mechanism was unheard of in previous attempts to organize the U.S. Government security structure. The process of policy development now moves at a much quicker speed and enjoys government-wide "buy-in" by member agencies and departments.

- The process of streamlining policy development could not be accomplished without first reducing and revamping the security policy structures that operated within the government. Once there were eight organizations for developing policy relating to the protection of facilities; we now have the Overseas Security Policy Board responsible for the overseas facilities such as U.S. embassies and consulates that under the Chief of Missions, and the Board responsible for all other aspects of U.S. security policy. Once there were two personnel security policy organizations, there is now one. There has never been a government-wide organization with the mission to standardize, professionalize, and modernize security training and professional development within the government; there is now one. The information Security Oversight Office (ISOO) and Classification Management Committee (CMC) of the Board have forged a close partnership to reform classification and safeguarding procedures. A Policy Integration Committee has been established to focus on overarching issues such as security costs and risk management as well as the eradication of redundancy among similar security programs. Close liaison and cooperative efforts have been established with the Overseas Security Policy Board, the National Counterintelligence Policy Board and the National Counterintelligence Center.

Consultations with these organizations occur as warranted during the policy development process.

- The Board and is subordinate structure has adopted the findings of the JSC to serve as the initial blueprint for needed reform During 1995, the Board has completed 20 percent of the 76 recommendations from the JSC. In total, the Board is currently addressing 114 distinct actions encompassing a wide range of security issues and priorities.
- The greatest challenge to confront the Board has been in the area of information systems security. The Board found well-intentioned, but fragmented groups, committees, panels, and boards, each trying to deal with some particular aspect or subset of Information Systems Security and closely-related Defensive Information Warfare. Recently, the Board Staff and the senior leadership of the Information Infrastructure Task Force Security Issues Forum, began sponsoring a series of meetings between representatives of the Civil and DoD/Intelligence Communities. The goal of these meetings is to advance mutual understanding of the topic, identify commonalties between the classified and unclassified systems and their vulnerabilities, and to come to an agreement on the these issues are to be addressed..
- The Board and its underlying committee structure has made significant strides in eliminating the fragmentation that exists in the security policy of the nation. By mobilizing 27 federal agencies and departments, with industry's advice and counsel, unified policy is being developed that:
  - is based on sound risk management;
  - is in consonance with the overall goals established in PDD-25;
  - takes into account the diverse threats our nation now faces, and;
  - recognizes a renewed interest and respect for the public's right to know.



Security Policy Forum

Personnel Security
Chair Pete Nelson
(OSDC3I)

Automation
Chair: Commerce

Financial Disclosure
Chair: C3I

Polygraph
Chair: NSA

Research and
Development
Chair: DOE

Facilities
Protection
Chair: Dave Schachnovsky
(NSA)

Access Control
Chair: NSA

Technical Security
Chair: NSA

Technical Training
Chair: NRO

Telephone Security
Chair: NRO

Security Protective
Force
Chair: DOE

Biometrics
Consortium
Chair: NSA

Research and
Development
Chair: DOE

Policy
Integration
Chair: Peter Saderholm
(SPBS)

International
Chair: OADTUSD(P)

NSDD 298 Review
Chair: Treasury

Security Cost
Estimations
Chair: SPBS

Safegaurds
Chair: Justice, DIA

Training and
Professional
Development
Chair: Dan McGarvey
(NRO)

Standards and
Professional Dev.
Chair: NSA

Security Awareness
and Education
Chair: FBI

Information Systems
Security Training
Chair: DISA/NCS

OPSEC and
Risk Management
Chair: IOSS

Classification
Management
Chair: Steve Garfinkle
(ISOO)

Standard Forms
Chair ISOO

Declassification
Chair: ISOO

* Not Established

Information Systems
Security*

United States Security Policy Board

Information Assurance Document Review Group

Organization: Security Policy Board Information Assurance Document (SPB IAD) Review Group/Working Group

Senior Information Warfare Official:

Peter D. Saderholm, Director, USSPB Staff

Information Warfare Points of Contact:

Vicki A. LaBarre, USSPB Staff

On-Line Resources:

Information Warfare Related Missions and Functions:

The Director of the US Security Policy Board Staff committed to the production of the Security Policy Board Information Assurance Document (IAD) No. 1 within the first six months of calendar year 1996. This document will be an attempt to provide requirements to assure the confidentiality, availability, and integrity of information systems. Industry's counsel on this matter is considered critical and, they are being included in the dialogue. The Director initiated the development of this document by the Staff due to absence of a standing committee concerned with the security of information systems reporting to the Forum,

The proposed INFOSEC policy under development by this working group will attempt to address INFOSEC in an innovative manner by encompassing the changing security and properties of data as it moves through networks, from system to system, through all of its states of transmission, processing, and storage.

Information Warfare Activities, Issues, Best Practices, Lessons Learned:

- On 29 March 1966, the Drafting Group successfully concluded the first draft of IAD No. 1. The draft was presented to the Review Group which includes representatives from all 27 departments/agencies/military services, as well as industry. Subsequent draft and reviews will be based on the perceived acceptability and utility of the document. As far as practical, every question brought up by the Review Group will be answered by the Drafting Group, either by inclusion in the next draft or by written reply. The goal is to provide, by early summer 1996, a completed and coordinated document for review by the Security Policy Forum.

This page intentionally left blank.

Advisory Committees

Advisory Committees

This page intentionally left blank.

Committee of Advisors on Science and Technology

Organization: Committee of Advisors on Science and Technology

Senior Information Assurance Official:

Information Assurance Points of Contact:

On-Line Resources:

Committee Homepage: http://www.whitehouse.gov/WH/EOP/OSTP/NSTC/html/pcas.html

Information Assurance Related Missions and Functions:

President Clinton established the President's Committee of Advisors on Science and Technology (PCAST) by Executive Order 12882 at the same time that he established the NSTC. The PCAST serves as the highest level private sector advisory group for the President and for the NSTC. The Committee members are distinguished individuals appointed by the President, and are drawn from industry, education and research institutions, and other non-governmental organizations. The Assistant to the President for Science and Technology co-chair the Committee with a private sector member selected by the President.

The formal link between the PCAST and the NSTC ensures that national needs remain an overarching guide for the NSTC. The PCAST provides feedback about Federal programs and actively advises the NSTC about science and technology issues of national importance.

Information Assurance Activities, Issues, Best Practices, Lessons Learned:

Computer System Security and Privacy Advisory Board

Organization: Computer System Security and Privacy Advisory Board

Senior Information Assurance Official:

Dr. Willis Ware, Chairman, RAND

Information Assurance Points of Contact:

Ed Roback, Board Secretary, National Institute for Standards and Technology

On-Line Resources:

CSSPAB Homepage: http://crsc.nist.gov/csspab

Information Assurance Related Missions and Functions:

In accordance with the requirements of Section 3 of the Computer Security Act of 1987 (P.L. 100-235), the Secretary of Commerce established the Computer System Security and Privacy Advisory Board, pursuant to the Federal Advisory Committee Act.

The Computer Security Act specifies that the Board's mission is to identify emerging managerial, technical, administrative, and physical safeguard issues relative to computer systems security and privacy.

The Board examines those issues affecting the security and privacy of sensitive unclassified information in federal computer and telecommunications systems. The Board's authority does not extend to private-sector systems or federal systems which process classified information.

The Board advises the Secretary of Commerce and the Director of the National Institute of Standards and Technology (NIST) on computer security and privacy issues pertaining to sensitive unclassified federal computer systems. The Board reports its findings to the Secretary of Commerce, the Director of the Office of Management and Budget, the Director of the National Security Agency, and appropriate committees of Congress.

NIST personnel serve as the Board's Secretariat. Other federal agency personnel may also assist the Board's activities as specified in the Computer Security Act of 1987.

The membership of the board includes: four members outside the Federal government eminent in the computer or telecommunications industry, including at least one representative of small or medium sized companies in such industries; four members from outside the Federal government who are eminent in the fields of computer or telecommunications technology, or related disciplines, but who are not employed or representatives of a producer of computer or telecommunications equipment; and four members from the Federal government, including one from the National Security Agency, who have computer systems management experience, including experience in computer systems security and privacy.

The Board reports through the Director of the National Institute of Standards and Technology to the Secretary of Commerce, and as required by Section 3 of the Computer Security Act of 1987, to the Director of the Office of Management and Budget, the Director of the National Security Agency, and the appropriate committees of the Congress. Members include:

Dr. Willis Ware (Chairman)
Computer Research Staff
RAND

Mr. Charlie Baggett
National Security Agency

Ms. Genevieve Burns
American Express Travel Related Services Company, Inc.

Mr. Addison Fischer
Fischer International Systems Corporation

Ms. Sandra Lambert
Lambert and Associates

Mr. Joseph Leo
U.S. Department of Agriculture

Ms. Gloria Parker
Department of Education

Mr. Randolph Sanovic

Mr. George Spix
Microsoft Corporation

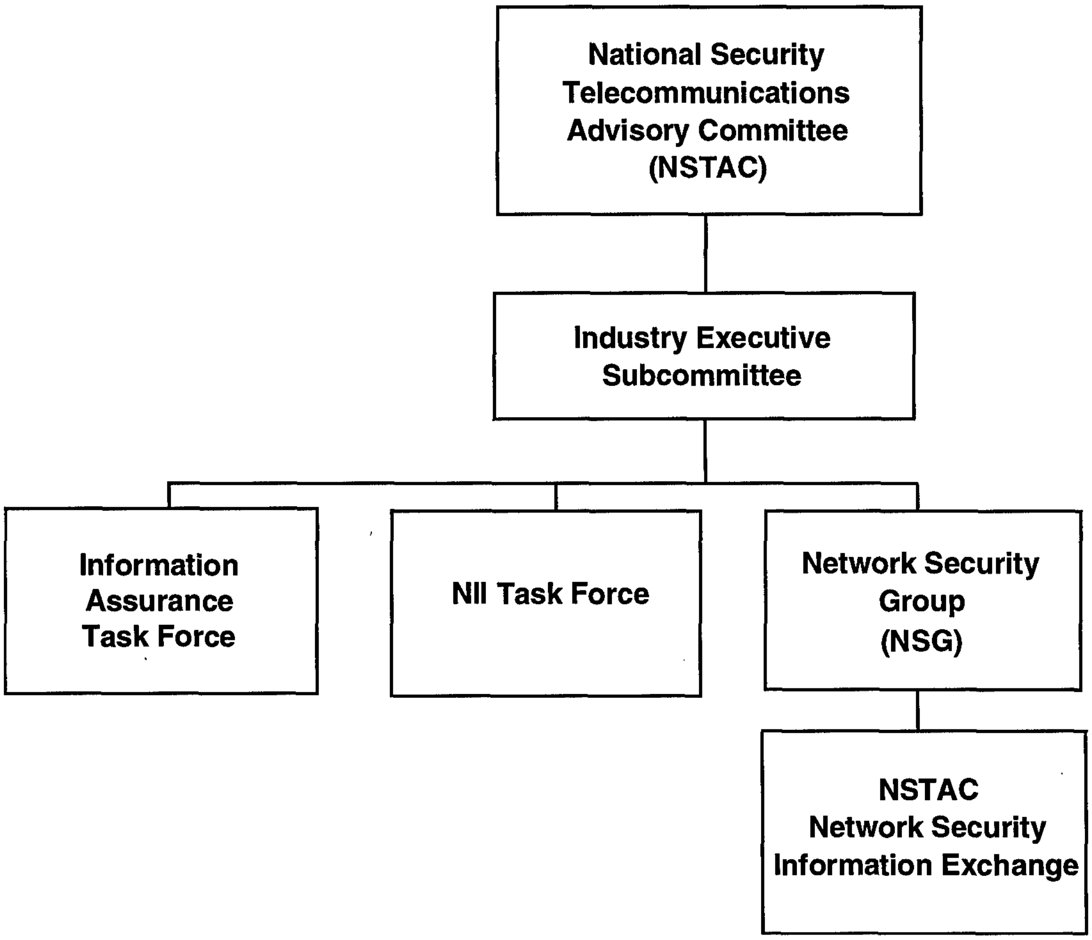
Ms. Linda Vetter

Mr. Frederick Weingarten
Computing Research Association

Mr. Bill Whitehurst
International Business Machines Corporation

Information Assurance Activities, Issues, Best Practices, Lessons Learned:

- The Board meets three to four times per year. The Board receives extensive updates and comments on on-going security and privacy activities throughout the Federal government and the private sector. The Board has been focusing on the following topics:
  - Encryption legislation and policy
  - Encryption products (government and commercial)
  - Key escrow
  - Common criteria for information technology security evaluation
  - Emerging security policy and implementation (e.g., Revised Appendix III to OMB Circular A-130)
  - Computer security lessons learned


National Security Telecommunications Advisory Committee (NSTAC)
Industry Executive Subcommittee
Information Assurance Task Force
NII Task Force
Network Security Group (NSG)
NSTAC Network Security Information Exchange

Organization: National Security Telecommunications Advisory Committee

Senior Information Assurance Official:

Information Assurance Points of Contact:

Fred Herr, Office of the Manager, National Communications Systems

On-Line Resources:

NSTAC Homepage: http://164.117.147.223/~ncs/html/nstac.html

Information Assurance Related Organizations, Missions and Functions:

E.O. 12382 established the President's National Security Telecommunications Advisory Committee (NSTAC) to provide advice and information from the perspective of industry to the President and the Executive Branch with respect to national security telecommunications policy and enhancements to NS/EP telecommunications.

Current NSTAC members are:

- ATCD
- AT&T Corporation
- Bank of America
- Bell Communications Research, Incorporated
- The Boeing Company
- Communications Satellite Corporation
- Computer Sciences Corporation
- CST
- Electronic Data Systems
- GTE Corporation
- Hughes Aircraft Company
- International Business Machines Corporation
- Interdigital
- ITT Corporation
- Lockheed-Martin
- Loral Corporation
- MCI Communications Corporation
- MFS Communications Company, Inc.
- Motorola, Incorporated
- Northern Telecom, Incorporated
- Pacific Telecom, Incorporated
- Rockwell International Corporation
- Science Applications International Corporation
- Sprint Corporation
- Teledisic
- TRW, Incorporated
- Unisys Corporation
- Telephone Association
- West, Incorporated
- WorldCom

Information Assurance Activities, Issues, Best Practices, Lessons Learned:

Wireless Services Task Force (WSTF)

- The WSTF is charged with:
  - Supporting Federal government efforts to implement Cellular Priority Access Service (CPAS). Provide advice, assist in dealing with standards and other industry bodies, support CPAS implementation activities with users and service providers, and participate in joint meetings. (CPAS would provide call-by-call priority access service for cellular radio.)
  - Determining the NS/EP implications and identifying the future task force involvement in the following emerging wireless systems and report to IES:
    * Land Mobile Radio/Specialized Mobile Radio (LMR/SMR)
    * Mobile Satellite Services (MSS)
    * Personal Communications Services (PCS)
    * Mobile Wireless Access to Data Networks
- The WSTF issued an Emerging Wireless Services Report. The report concluded that:
  - NS/EP telecommunications capabilities could benefit from a joint industry-government investigation of the use of new wireless technologies in NS/EP operations.
  - It would be beneficial for Federal, State, and local representatives to collaborate on NS/EP issues involved in new and evolving wireless technologies.
- In addition, the report recommended that the Government should:
  - Define and establish unified policies and requirements for wireless services in support of NS/EP activities at Federal, State and local levels.
  - Identify NS/EP issues inherent in emerging technologies to include providing NS/EP orientation to newly involved entities.
  - Identify interoperability and security constraints inherent in emerging wireless technologies and determine alternative solutions.
  - Identify approaches to providing end-to-end network privileges for NS/EP users associated with these new technologies.

NII Task Force

- The NII Task Force was established in August 1993 to provide the President guidance on the types of government policies, programs, and applications that should be implemented to ensure N/SEP requirements are satisfied in the evolving NII.
- Most recently the NII Task Force has addressed three charges from NSTAC XVII:
  - Determine the need for and, if found appropriate, develop a proposed charter for an NII Security Center of Excellence (SCOE)
  - Determine the NS/EP implications of the emerging global information infrastructure (GII)
  - Complete a current assessment and report on emergency health care information issues.

- With regard to these charges the NII Task Force concluded that:
  - A national level organization (SCOE) is needed to address unmet NII security functions: adoption of security evaluation standards and techniques; coordination in the development of standards; development and promulgation of methodologies for testing and rating security products and services; education of private, corporate, organizational and government users, providers, and decision makers.
  - Furthermore, the SCOE model should be private sector-based, privately funded, and include users, providers, professional associations, and vendors. Also, an Information Systems Security Board (ISSB), based on the Financial Accounting Standards Board (FASB) model, could perform the security functions identified by the task force.
  - The U.S. Government, in conjunction with other governments and U.S. telecommunications and information industries, should continue to define, sponsor, and participate in international projects that raise technology and policy issues critical to the evolution of the GII.
  - The IES, in cooperation with the U.S. Government, should address the increasing NS/EP threat to the NII resulting from the evolving GII.
  - With regards to Emergency Health Care Information, the President should urgently ensure that ongoing activities (e.g., those in response to PDD 39) are coordinated to do the following:
    - * Develop and maintain integrated plans, including emergency communications, to ensure that existing and evolving NII capabilities can support a coordinated emergency medical response to nuclear/biological/chemical incidents or similarly catastrophic events.
    - * Regularly exercise and evaluate response plans.
    - * Identify and examine other critical response infrastructures to determine if the emergency communications and information management issues found with emergency medical response are shared.
    - * Actively involve NSTAC in the review of the coordinated emergency plans.

Network Security Group

- The Network Security Group is charged with the following responsibilities:
  - Oversee NSTAC Network Security Information Exchange (NSIE)
  - Represent NSTAC on network security matters to the Manager, NCS, and the FCC's Network Reliability Council.
  - Participate in the research and development information exchange between government and industry.
- Recently, the Network Security Group has explored the concept of "middle-ground" security that should provide sufficient protection for the corporate and individual users while balancing the needs of the law enforcement and intelligence communities.

- Conducted NSIE Risk Assessment focusing on current and near-term public networks. The report concluded that:
  - Reliance on Public Networks is increasing.
  - Explosive growth of new types of service providers and new technology is increasing the complexity of the network and its interfaces, introducing new vulnerabilities.
  - Deterrent capabilities are improving, but have not kept pace with the threat.
  - Protection measures are improving, but have not kept pace with the vulnerabilities.
  - Risk to public networks is greater today than reported in 1993.
- Furthermore, the NSG Perspective on Risk notes that:
  - Current Federal computer crime laws are not fully effective.
  - Government and industry sponsored R&D is insufficient.
  - Nationwide indications, warnings and assessment capability does not exist.

Information Assurance Task Force

- The Information Assurance Task Force is conducting a Risk Assessment of the following infrastructures:
  - Electric generation, transmission, and distribution system (estimated completion date: fall 1996)
  - Financial system (estimated completion date: end 1997)
  - Transportation system (tentative completion date: summer 1997)

This page intentionally left blank.

Network Reliability and Interoperability Council

Organization: Network Reliability and Interoperability Council (NRIC)

Senior Information Assurance Official:

Information Assurance Points of Contact:

On-Line Resources:

Information Assurance Related Organizations, Missions and Functions:

The Network Reliability and Interoperability Council (NRIC) is a Federal Advisory Committee chartered by the Federal Communications Commission (FCC). The charter was renewed for a third two-year term beginning January 6, 1996. This advisory committee was first chartered in the spring of 1992 to investigate reliability of the public switched network after several service outages during 1990 and 1991 affected large numbers of users and an air traffic control system. During its first two terms the committee, then named the Network Reliability Council (NRC), recommended a system for common carrier reports to the FCC when service outages affect either a large number of users or critical facilities, such as major airports and important government locations. Implementation of reporting was expedited by using a voluntary process and was finalized by adoption of an FCC rule. [47 C.F.R. 63.100]

Members of the Council include Chief Executive Officers and other executives of major telecommunications common carriers, equipment suppliers, communications trade associations, research facilities, standards organizations, cable companies, computer industry firms, satellite companies, consumer organizations, communications employees, state regulators, and Federal government user representatives. Subordinate focus groups operate within an industry standards organization, the Alliance for Telecommunications Industry Solutions (ATIS), under the direction of the Network Reliability Steering Committee (NRSC). The focus groups are as follows:

Performance Metrics Team
Best Practices Team
Outage Reporting and Customer Notification Team
Increased Interconnection Task Group
Reliability Issues - Changing Technologies Focus Group:
  SONET/ATM
  New Wireless Technologies
  Satellite Communications Networks
  Wireless/PCS
  Advanced Intelligent Network
  Essential Communications During Emergencies
  Telecommuting as a Back-up in Emergencies

In June 1993 the Council published an extensive report of its work, "Network Reliability: A Report to the Nation," in fulfillment of its original charter and mission. Council findings had proven to be an effective basis for improvement of network reliability in the industry. It was therefor important to ensure that a broadly based committee of industry experts remained actively involved in further reducing the number of outages and their effect on users.

In renewing the charter for a second two year term, effective July 1994, the FCC requested the Council to: (1) evaluate the reliability of network services on a local and regional basis, (2) evaluate potential risks from new interconnection arrangements, (3) assess the impact of changing technologies including cable television and wireless, (4) evaluate access to emergency services during network outages, and (5) determine whether network outages have disproportionate impact on certain geographic areas or certain demographic groups. These functions continue into the following charter period.

A new charter, effective January 6, 1996, continues the Council during this era of deregulation, increasing competition, and rapid technological change. The Telecommunications Act of 1996, effective February 8, 1996, is a major revision of the Communications Act of 1934. The changes favor competition between existing telecommunications common carriers without geographic or territorial market distinctions. Competitive entry to the market is also eased for non-traditional providers including power, computer, railroad, cable television, satellite, and pipeline companies. The 1996 Act provides a legislative basis for Open Network Architecture (ONA) which is the unbundling of network and switched service elements. Existing FCC rules had established ONA, primarily to enable competitive access providers to interconnect their services to users through facilities of local exchange carriers. The 1996 Act includes requirements for all carriers to cooperate in ensuring interoperability of their services.

Members of the NRIC include:

Interexchange Carriers

AT&T
MCI Comm. Corp.
Sprint

Local Exchange Carriers
Ameritech
Bell Atlantic
Bell South
GTE Corporation
NYNEX Corporation
Pacific Telesis
Southwestern Bell
US West, Inc.
Rochester Telephone

Research and Standards Groups
Bell Communications Research (Bellcore)
Alliance for Telecommunications Industry Solutions (ATIS)
Cox Cable Communications, Inc. (Cable Labs)

Trade Associations
Association for Local Telecommunications Services (ALTS)
Competitive Telecommunications Association (COMPTEL)
Organization for the Protection and Advancement of Small Telephone Companies (PASTCO)
United States Telephone Association (USTA)
Telecommunications Industry Association (TIA)
National Cable Television Association (NCTA)
Cable Telecommunications Association (CATA)
Personal Communications Industry Association (PCIA)
Cellular Telecommunications Industry Association (CTIA)

Large Consumer Representatives
Ad Hoc Telecommunications Users Group
International Communications Association (ICA)

Small Consumer Representatives
Alliance for Public Technology
National Association of State Utilities Consumer Advocates (NASUCA)

Cable Companies
Time Warner Communications

Satellite Representatives
Hughes Space and Communications Company

Government Related Organizations
National Association of Regulatory Utility Commissioners (NARUC)
National Communications System

Labor
Communications Workers of America, AFL-CIO

Computer Firms
IBM

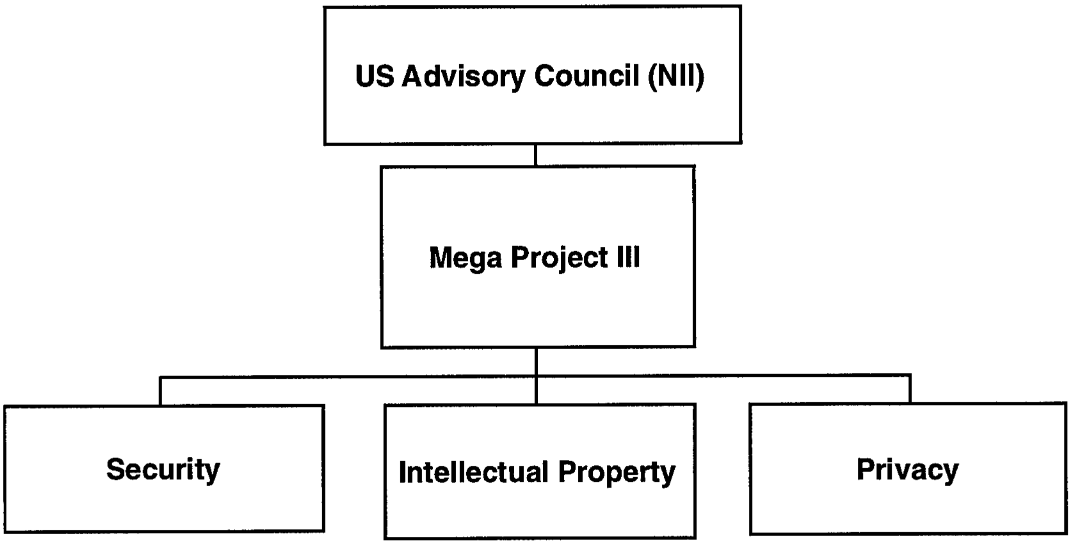
Observer Members

National Telecommunications and Information Administration, U.S. Department of Commerce

Office of Science and Technology Policy, White House

Information Assurance Activities, Issues, Best Practices, Lessons Learned:

This page intentionally left blank.


US Advisory Council (NII)
Mega Project III
Security
Intellectual Property
Privacy

Organization: United States Advisory Council on the NII

Senior Information Assurance Official:

N/A

Information Assurance Points of Contact:

Yvette Barrett, IITF Secretariat

On-Line Resources:

USAC Homepage: http://niiac-info.org/~niiac

Information Assurance Related Organizations, Missions and Functions:

Established by Executive Order No. 12864, the Advisory Council on the National Information Infrastructure (NII) was established to identify appropriate government action and advise the Secretary of Commerce, on matters related to the development of the NII. The Council members represented the many different stakeholders in the NII, including industry, labor, academic, public interest groups, and state and local governments.

Current members are:

Mr. Morton Bahr, President
Communications Workers of America, AFL-CIO
Dr. Toni Carbo Bearman, Dean and Professor,
School of Library and Information Science University of Pittsburgh
Ms. Marilyn Bergman
President, American Society of Composers, Authors, and Publishers (ASCAP)
Ms. Bonnie Laverne Bracey, Teacher
Ashlawn Elementary School, Arlington, Virginia
Mr. John F. Cooke, President
The Disney Channel
Ms. Esther Dyson, President
EDventure Holdings
Mr. William C. Ferguson, Chairman and Chief Executive Officer
NYNEX corporation
Dr. Craig Fields, Chairman and Chief Executive Officer
Microelectronics and Computer Technology Corporation
Mr. Jack Fishman, Publisher
Citizen-Tribune
Ms. Lynn Forester, President and Chief Executive Officer
Firstmark Holdings, Inc.

Honorable Carol Fukunaga, Senator
State of Hawaii
Mr. Jack Golodner, President
Department for Professional Employees, AFL-CIO
Mr. Eduardo Gomez, President and General Manager
KABQ Radio, Albuquerque, New Mexico
Mr. Haynes G. Griffin, President and Chief Executive Officer
Vanguard Cellular Systems, Inc.
Dr. George Heilmeier, President and Chief Executive Officer
Bellcore (Bell Communications Research)
Ms. LaDonna Harris, President
Americans for Indian Opportunity
Ms. Susan Herman, General Manager
Department of Telecommunications, City of Los Angeles
Mr. James R. Houghton, Chairman and Chief Executive Officer
Coming Incorporated
Mr. Stanley S. Hubbard, Chairman and Chief Executive Officer
Hubbard Broadcasting, Inc. and the United States Satellite Broadcasting Company, Inc.
Mr. Robert L. Johnson, Founder and President
Black Entertainment Television (BET)
Dr. Robert E. Kahn, President
Corporation for National Research Initiatives (CNRI)
Ms. Deborah Kaplan, Vice President
World Institute on Disability
Mr. Mitchell Kapor, Chairman
Electronic Frontier Foundation
Mr. Delano E. Lewis, President and Chief Executive Officer
National Public Radio (NPR)
Mr. Alex J. Mandl, Chief Executive Officer
Communications Services Group, AT&T
Mr. Edward R. McCracken, Chairman and Chief Executive Officer
Silicon Graphics, Inc.
Dr. Nathan Myhrvold, Senior Vice President of Advanced Technology
Microsoft Corporation
Mr. N.M. (Mac) Norton, Jr., Attorney-at-Law
Wright, Lindsey & Jennings
Mr. Vance K. Opperman, President
West Publishing Company
Ms. Jane Smith Patterson, Advisor to the Governor of North Carolina
for Policy, Budget and Technology
Ms. Frances W. Preston, President and Chief Executive Officer
Broadcast Music Incorporated (BMI)
Mr. Bert C. Roberts, Jr., Chairman and Chief Executive Officer
MCI Communications Corporation

Mr. John Sculley, Former Chairman
Apple Computers, Inc.
Ms. Joan H. Smith, Chairman
Oregon Public Utility Commission
Mr. Al Teller, Chairman and Chief Executive Officer,
MCA Music Entertainment Group
Mr. Lawrence Tisch, President and
Chief Executive Officer, CBS, Incorporated
Mr. Jack Valenti, Chief Executive Officer and President
Motion Picture Association of America

Information Assurance Activities, Issues, Best Practices, Lessons Learned:

- In January 1996, the Council issued its final report entitled "A Nation of Opportunity: Realizing the Promise of the Information Superhighway" and officially disbanded. Relevant highlights from the Council's report are extracted below.
  - "The United States stands today in the midst of one of the great revolutions in recorded history: the Information Age. The Information Superhighway provides the infrastructure that enables enormous benefits in education, economic well-being, and quality of life."
  - "Electronic Commerce. The Federal government, in conjunction with others, should take the steps to identify and resolve, wherever possible, legal, regulatory, and policy issues that would restrict the development of electronic commerce on the Information Superhighway."
  - "The Federal government should convene a broad-based committee composed of those entities involved in standard setting, those involved with the development of new technology, and relevant State, local, and Tribal agencies to meet the needs of the emergency management, public safety, and criminal justice communities."
  - "The Federal government should encourage private sector awareness of security issues, initiate a public-private security consultation process, and foster mechanisms to promote private accountability for proper use of security measures."
  - "The Federal government should not inhibit the development and deployment of encryption by the private sector."

This page intentionally left blank.

Independent Establishments and Government Corporations

Independent Establishments and Government Corporations

This page intentionally left blank.

Central Intelligence Agency J. Deutch

Organization: Central Intelligence Agency

Senior Information Warfare Official:

John Deutch, Director of Central Intelligence
RADM Dennis Blair, Associate Director of Central Intelligence for Military Support

Information Warfare Points of Contact:

Chief, Critical Defense Technologies Division, Office of Weapons, Technology, and Proliferation
Chief, Information Warfare Brranch (CTD, OWTP)

On-Line Resources:

CIA Homepage: http://www.odci.gov/cia/

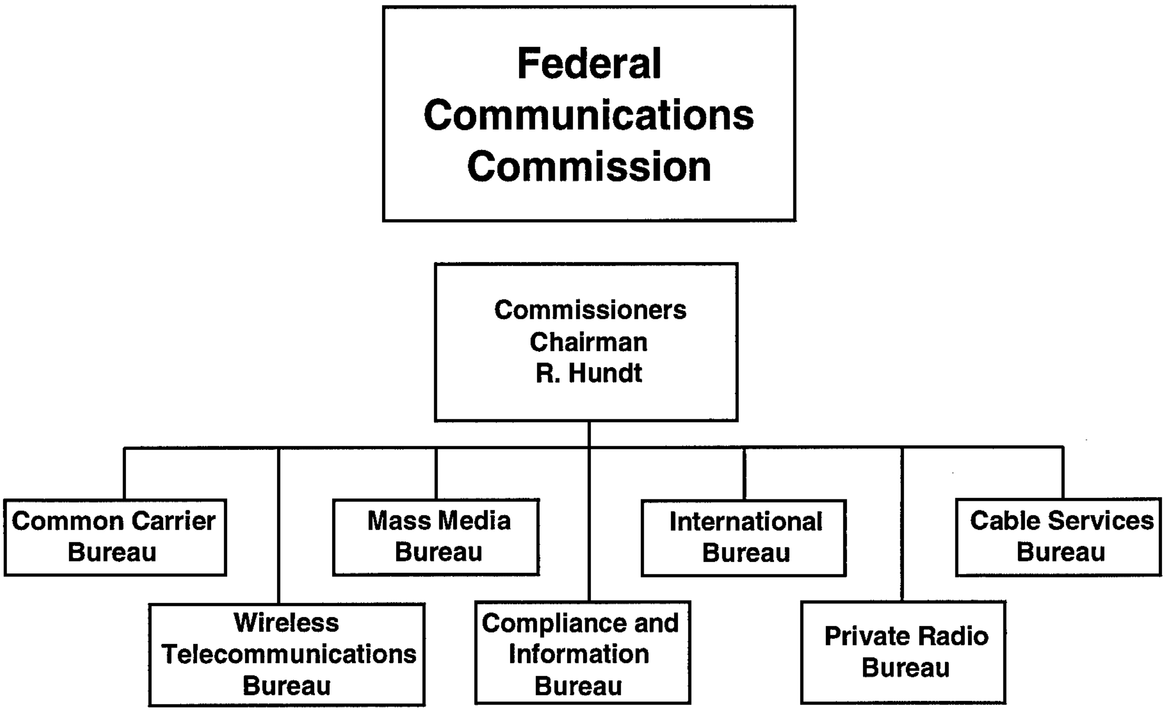
Information Warfare Related Missions and Functions:

Overall policy and tasking for the Intelligence Community in general, and for the CIA in particular, to supply foreign intelligence support to the U.S. government on information warfare issues and activities.

The Office of Weapons, Technology, and Proliferation (OWTP) focuses on scientific and technical intelligence on foreign military R&D and system development and acquisition. The Critical Defense Technologies Division has been tasked with looking at new technology development and related acquisition programs for information system technologies, inter alia.

Information Warfare Activities, Issues, Best Practices, Lessons Learned:

- This is a relatively new thrust for the Intelligence Community, and they have just begun to adjust to deal with this "new" warfare area.


Federal Communications Commission
Commissioners
Chairman
R. Hundt
Common Carrier Bureau
Wireless Telecommunications Bureau
Mass Media Bureau
Compliance and Information Bureau
International Bureau
Private Radio Bureau
Cable Services Bureau

Organization: Federal Communications Commission (FCC)

Senior Information Assurance Official:

Vacant, Defense Commissioner

Information Assurance Points of Contact:

Arlan Van Doorn, Deputy Chief, Compliance and Information Bureau, Representative to the NCS Committee of Principals
Roy Kolly, Compliance and Information Bureau, Representative to the NCS Council of Representatives
Herbert Neumann, Common Carrier Bureau, Representative to the NCS National Coordinating Center for Telecommunications

On-Line Resources:

http://www.fcc.gov/

Information Assurance Related Missions and Functions:

The Federal Communications Commission regulates, licenses and monitors the operation of communications services to ensure reliable and competitive nationwide and international communications. The services regulated include broadcast (radio and television), telephone, wireless (cellular, PCS, satellite), and other digital and analog applications. Transmission facilities include radio, wire, cable, light-guide and satellite. FCC functions include ensuring that communications capabilities are provided for the promotion of life and property and for the national defense.

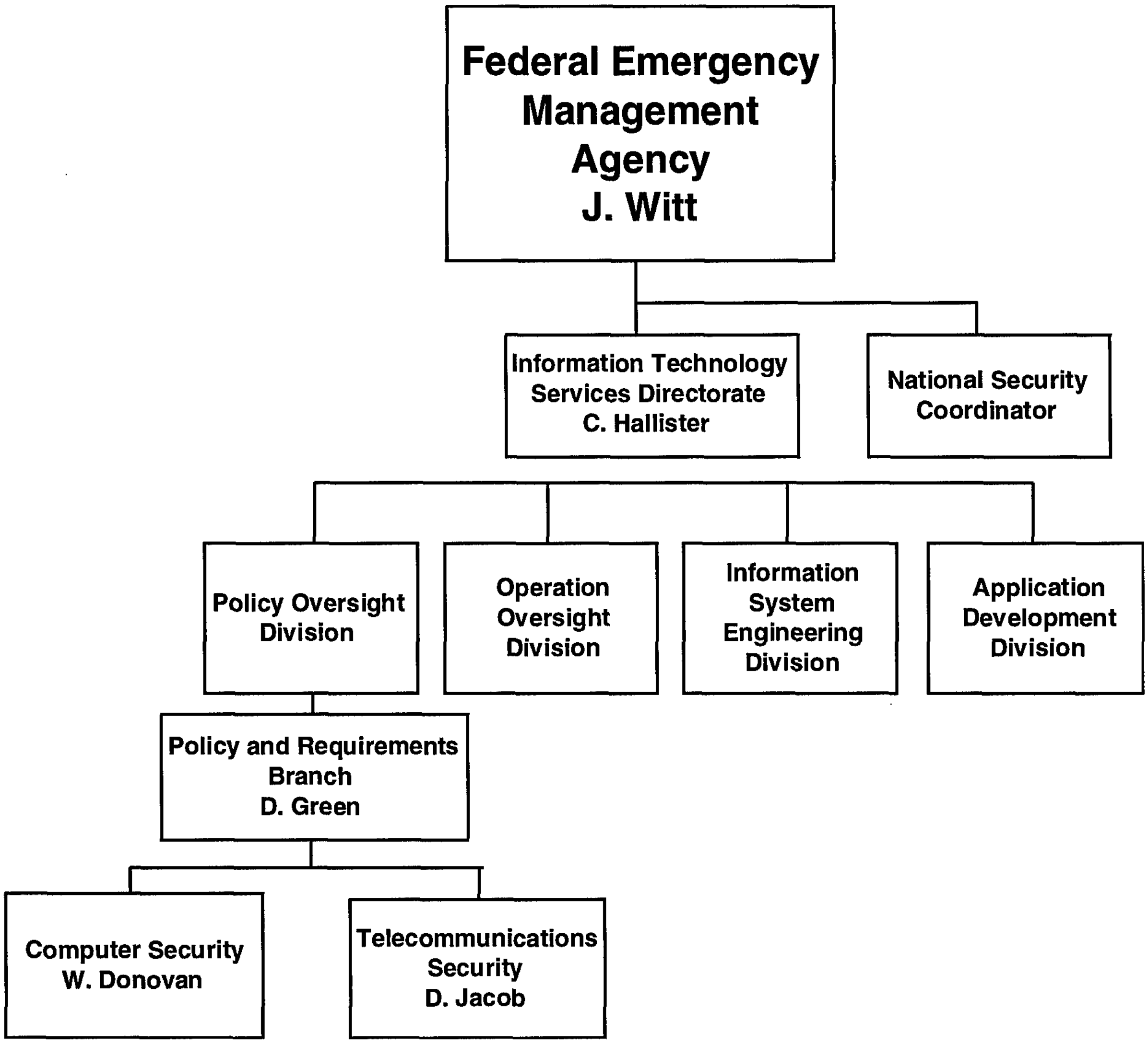
The Commission uses a combination of required reports and its own investigation to monitor performance of licensees. In the telecommunications area, a Federal Advisory Committee, now designated the Network Reliability and Interoperability Council (NRIC), was chartered in 1992 to investigate reliability of the public switched network after the occurrence of several major service outages. The NRIC recommended a system of common carrier reports which the Commission adopted (47 C.F.R. 63.100). Reports are required from any common carriers that experiences a service outage that affects either 30,000 potential users for at least 30 minutes or when an outage impacts a major airport (as defined by the FAA), a major government or military facility, a nuclear power plant, or an emergency 911 tandem switch. Outages involving nuclear power plants, government facilities and military facilities are reported through the NCS National Coordinating Center (NCC). The initial report is made to the DISA Network Management Operations Center which contacts NCC staff members. NCC staff members evaluate the impact and report it to the FCC Watch Officer, if appropriate. Other outages are reported directly to the FCC Watch Officer in Washington, DC. A backup reporting location is also available. Telephonic reports are followed by hard copy reports and final reports are due within 30 days. The telecommunications industry has used the NRIC as an effective vehicle for cooperation in improving network reliability and resiliency. An organizational summary of the NRIC can be found under Advisory Committees in this appendix.

The FCC is required to issue rules to enable implementation of the Telecommunications Act of 1996. This Act, effective February 8, 1996, is a major revision of the Communications Act of 1934. The changes favor competition between existing telecommunications common carriers without geographic or territorial market distinctions. Competitive entry to the market is also eased for non-traditional providers including power, computer, railroad, cable television, satellite, and pipeline companies. The 1996 Act provides a legislative basis for Open Network Architecture (ONA) which is the unbundling of network and switched service elements. Existing FCC rules had established ONA, primarily to enable competitive access providers to interconnect their services to users through facilities of local exchange carriers. The 1996 Act includes requirements for all carriers to cooperate in ensuring interoperability of their services.

Information Assurance Activities, Issues, Best Practices, Lessons Learned:

- The primary concern of the FCC and the common carrier industry is network reliability, rather than security of the information carried.
- Carriers have initiated Mutual Aid Agreements in an effort to reduce the impact of service disruptions.
- Industry standards work may result in greater information security because of the shrinking distinction between network control data and message data.
- Network reliability has been improved through addition of geographically diverse multiple routes; use of improved technology, such as self-healing fiber optic ring architecture; and rapid computer controlled rerouting of large circuit groups around network damage, such as a cable cut.
- FCC is a member of the joint government and industry Network Security Information Exchange (NSIE) whose function is to share sensitive information that can be used to counter illegal use of telecommunications to: (1) disrupt service, (2) commit fraud, (3) gain unauthorized access to computers, (4) commit acts of espionage and, (5) engage in other criminal activities. The NSIE is further discussed in the organizational summary of the NSTAC.

This page intentionally left blank.



Federal Emergency Management Agency
J. Witt

Information Technology Services Directorate
C. Hallister

National Security Coordinator

Policy Oversight Division

Operation Oversight Division

Information System Engineering Division

Application Development Division

Policy and Requirements Branch
D. Green

Computer Security
W. Donovan

Telecommunications Security
D. Jacob

Organization: Federal Emergency Management Agency (FEMA)

Senior Information Assurance Official:

Clay G. Hollister, Associate Director, Information Technology Services Directorate (ITSD)

Information Assurance Points of Contact:

Dennis B. Green, Chief, Oversight Branch, Policy and Oversight Division, ITSD
William W. Donovan, Information System Security, Oversight Branch, Policy and Oversight Division, ITSD

On-Line Resources:

FEMA Homepage: http://www.fema.gov/

Information Assurance Related Missions and Functions:

The Federal Emergency Management Agency (FEMA) is the central agency within the Federal government for emergency planning, preparedness, mitigation, response, and recovery. FEMA funds emergency programs, offers technical guidance and training, and deploys Federal resources in time of catastrophic disaster. FEMA is also responsible for developing plans to ensure the continuity of the Federal government during national security emergencies, and Federal response to the consequences of major terrorist incidents.

FEMA is an independent federal agency with more than 2,400 full time employees: at FEMA headquarters in Washington, DC, at regional and area offices across the country, at the Mount Weather Emergency Assistance Center, and at the FEMA training center in Emmitsburg, Maryland. FEMA also has nearly 4,000 standby disaster assistance employees who are available to help out after disasters. Often FEMA works in partnership with other organizations that are part of the nation's emergency management system. These partners include state and local emergency management agencies, 27 federal agencies and American Red Cross.

Information Assurance Activities, Issues, Best Practices, Lessons Learned:

- The Information Technology Services consolidates most of the information systems development and operational activities from throughout the Agency.
- An unclassified February 28, 1995, NSC memorandum states it is the policy of the Administration to continue the preparedness activities cited in Executive Order 12656, Assignment of Emergency Preparedness Responsibilities, November 23, 1986. It further states that "Natural disasters and other emergencies, which may cause widespread or prolonged disruption of critical Federal government functions, also warrant continued consideration as potential national security challenges" and that responsibilities "involve preparedness for any occurrence, including natural disaster, military attack, technological

emergency or other emergency that seriously degrades or seriously threatens the national security." Finally, the memorandum charges FEMA with preparing "an assessment of the existing continuity of operations and continuity of government programs."

- FEMA information assurance activities are not fully developed because of budget and emphasis on response to natural and man-made disasters.
- Absolutely need an Executive Order to assign responsibilities in this area. Policy must include consequences for not following the policy. Health and Safety analog should be reviewed for possible application to the information area.
- Training and education regarding information assurance should be integrated into other training. In addition, this training should be mandatory. Senior leadership awareness, interest, and support is absolutely required! With size of government and the budget decreasing, we must emphasize awareness.
- Suggested forming a Federal government organization which could provide advice and assistance regarding solutions to security problems. This organization should be centrally funded. NIST currently evaluates products but has restrictions on what information can be released to the government at large.
- Bare-bones internal information security policies are in place. Efforts are underway to improve existing policies.
- Donovan is the lone person responsible for developing and implementing computer security for FEMA.
- The Federal Emergency Management Agency's Federal Response Plan (for Public Law 93-288, as amended) describes FEMA's Concept of Operations to address the consequences of any disaster or emergency situation in which there is a need for Federal response assistance under the authorities of the Stafford Act. It is applicable to natural disasters; technological emergencies involving radiological or hazardous material releases; and other incidents requiring Federal assistance under the Act. The Response Plan describes the basic mechanisms and structures by which the Federal government will mobilize resources and conduct activities to augment State and local response efforts. To facilitate the provision of Federal assistance, the Plan uses a functional approach to group the types of Federal assistance which a State is most likely to need under twelve Emergency Support Functions (ESFs). Each ESF is headed by a primary agency, which has been selected based on its authorities, resources and capabilities in the particular functional area. Other agencies have been designated as support agencies for one or more ESF based on their resources and capabilities to support the functional area. The twelve ESFs serve as the primary mechanism through which Federal response assistance will be provided to assist the State in meeting response requirements in an affected area. Federal assistance will be provided to the affected State under the overall coordination of the Federal Coordinating Officer (FCO) appointed by the Director of FEMA on behalf of the President. Federal assistance provided under P.L. 93-288, as amended, is to supplement State and local government response efforts. ESFs will coordinate with the FCO and the affected State to identify specific response requirements and will provide Federal response assistance based on State-identified priorities. Each ESF will provide resources using its primary and support agency authorities and capabilities, in coordination with other ESFs, to support its missions. ESFs will allocate available resources to each declared State based on priorities identified in conjunction with the State and in coordination with the

FCO. If resources are not available within the declared State, the ESF will seek to provide them from a primary or support agency area or region. If the resource is unavailable from an area or region, the requirement will be forwarded to the appropriate ESF headquarters office for further action. One or more disasters may affect a number of States and regions concurrently. In those instances, the Federal government will conduct multi-State response operations; for each declared State, an FCO will be appointed to coordinate the specific requirements for Federal response and recovery within that State. Under multiple State declarations, ESF departments and agencies will be required to coordinate the provision of resources to support the operations of all of the declared States. The following are the primary agencies for the Emergency Support Function listed:

Emergency Support Function	Primary Agency
1. Transportation	Department of Transportation
2. Communications	National Communications System
3. Public Works and Engineering	U.S. Corps of Engineers (DoD)
4. Firefighting	Forest Service (USDA)
5. Information and Planning	Federal Emergency Management Agency
6. Mass Care	American Red Cross
7. Resource Support	General Services Administration
8. Health and Medical Services	Public Health Service (DHHS)
9. Urban Search and Rescue	Department of Defense
10. Hazardous Materials	Environmental Protection Agency
11. Food	U.S. Department of Agriculture
12. Energy	Department of Energy

Federal Reserve System

Organization: Federal Reserve System (FRS)

Senior Information Assurance Official:

For Federal Reserve Banks:
Clyde H. Farnsworth, Jr., Director, Division of Reserve Bank Operations and Payment Systems

For Board of Governors:
Steven R. Malphrus, Division of Information Resources

Information Assurance Points of Contact:

John H. Parrish, Assistant Director, Division of Reserve Bank Operations and Payment Systems
Kenneth D. Buckley, Manager, Division of Reserve Bank Operations and Payment Systems
Raymond Romero, Project Leader, Division of Reserve Bank Operations and Payment Systems

On-Line Resources:

Federal Reserve Banks: http://www.frbatlanta.org/main/frbsites.htm

Information Assurance Related Missions and Functions:

The Federal Reserve System is the central bank of the United States. It is charged by Congress with responsibility for conducting the nation's monetary policy; supervising and regulating banking institutions; maintaining the stability of the financial system; and providing certain financial services to the U.S. government, financial institutions, and foreign central banks. The Federal Reserve is also responsible for promoting efficiency in payment system practices.

In carrying out these responsibilities, the Federal Reserve executes monetary policy, examines commercial banks, transfers funds and government securities, handles government deposits and debt issues, acts as the lender of last resort, and a wide range of other activities. The System consists of seven parts: the Board of Governors, the twelve Federal Reserve Banks and their twenty-five branches, the Federal Open Market Committee, the Federal Advisory Council, the Consumer Advisory Council, the Thrift Advisory Council, and depository institutions.

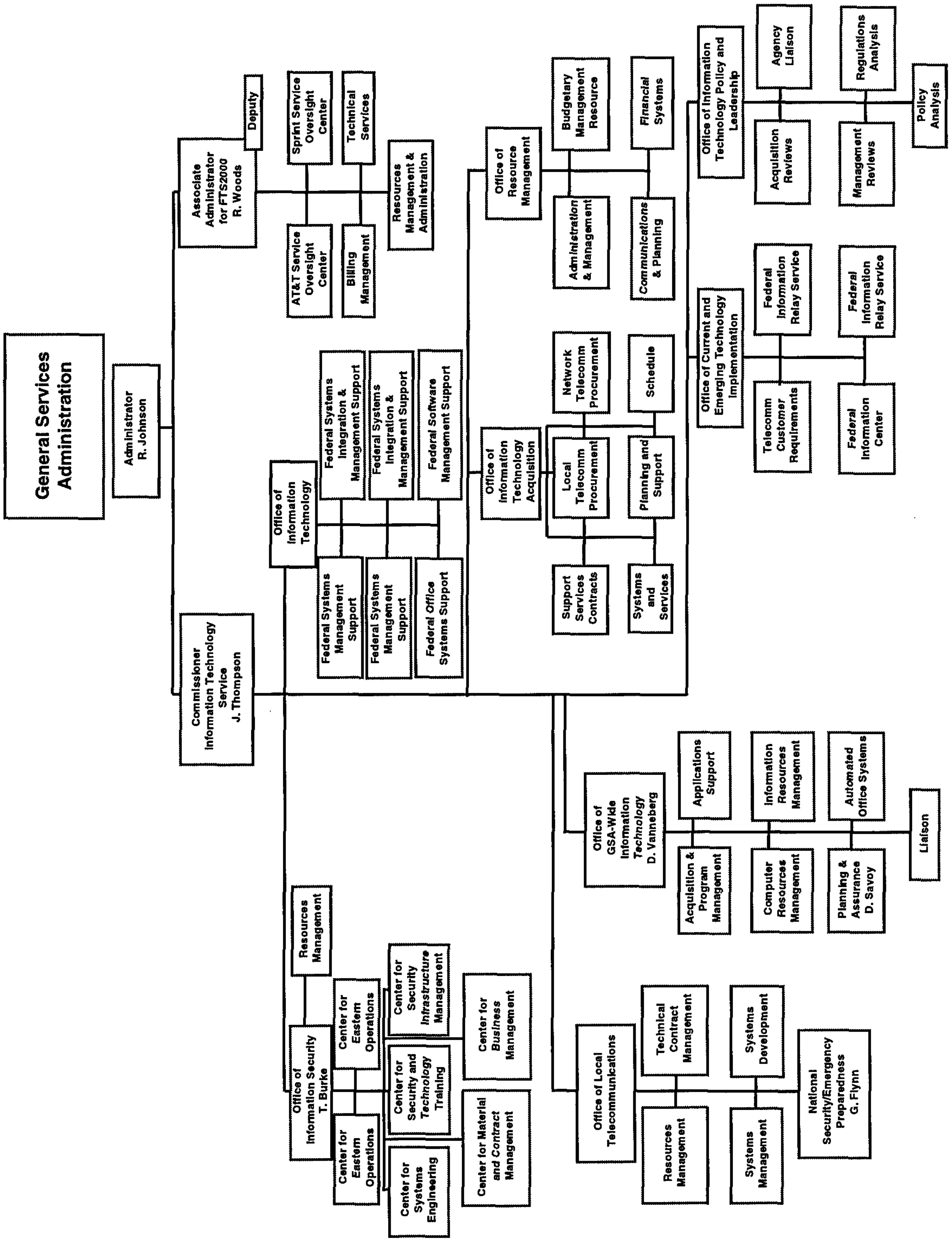
The Board of Governors exercises general supervision over Reserve Bank activities and examines each Reserve Bank annually. The Board approves minimum standards for data security in Reserve Banks, and the effectiveness of the Banks' implementation of controls is evaluated during the annual examinations and during internal audits.

The Board of Directors of each Federal Reserve Bank is composed of nine members: three represent the stockholding member banks and are elected by those banks; three represent commerce, agriculture, or industry in the district and are elected by the stockholding member banks; and three are appointed by the Board of Governors. The Board of Governors appoints one of these latter directors as Chairman of the Board of Directors and another as the Deputy Chairman.

Information Assurance Activities, Issues, Best Practices, Lessons Learned:

- FRS was created as the Central Bank of the U.S. by act of Congress and is independent within government. Many checks and balances are used to oversee bank operations and maintain the integrity of the System. Parrish's office in the Division of Reserve Bank Operations and Payment Systems is responsible for advising the Board of Governors on the information security aspects of Reserve Bank operations.
- The Chief Operating Officers of each Federal Reserve Bank form a committee to deal with the many aspects of the FRS operation. The committee has in turn formed several working groups to deal with specialized and technical aspects of the FRS operation. One of these working groups is made up of the data security officers of each Federal Reserve Bank. This working group is responsible for developing and recommending security policy. The full committee approves the security policy which is implemented only with the concurrence of the Reserve Bank Operations and Payment Systems, acting on behalf of the Board of Governors.
- Each Federal Reserve Bank conducts internal audits, which include security reviews.
- The Board of Governors examines the Federal Reserve Banks on an annual basis. The Division of Reserve Bank Operations and Payment Systems has oversight responsibility with respect to the security operations of the Federal Reserve Banks.
- Recognition of the public responsibilities of the central bank drive a long-time organizational emphasis on integrity and effective controls in operations. Ownership of and accountability for information, need to know, separation of control, and custody of information procedures have been in place for decades to preserve that integrity. As manual procedures for processing physical valuables were automated over the years, appropriate controls were established for processing in the electronic environment.
- FRS operates three primary data centers and has extensive backup capabilities in the event of partial or whole site failures. Full disaster recovery plans are in place.
- FedWire is the real-time payments system application which provides over $200 trillion in funds transfer and government securities transactions between financial institutions a year. FedNet is the FRS network over which this traffic moves. Fedline is the link between financial institutions and FedWire.
- The Federal Reserve also oversees the Clearing House for Interbank Payments (CHIPS). This is a private sector multilateral net settlement clearing system operated by the New York Clearing House Association in New York City. It clears over $1 trillion a day.

This page intentionally left blank.


General Services Administration
Administrator R. Johnson
Associate Administrator for FTS2000 R. Woods
Deputy
Sprint Service Oversight Center
Technical Services
Resources Management & Administration
AT&T Service Oversight Center
Billing Management
Commissioner Information Technology Service J. Thompson
Office of Information Technology
Federal Systems Integration & Management Support
Federal Systems Integration & Management Support
Federal Software Management Support
Federal Systems Management Support
Federal Systems Management Support
Federal Office Systems Support
Office of Information Technology Acquisition
Network Telecomm Procurement
Schedule
Local Telecomm Procurement
Planning and Support
Support Services Contracts
Systems and Services
Office of Resource Management
Budgetary Management Resource
Financial Systems
Administration & Management
Communications & Planning
Office of Information Technology Policy and Leadership
Agency Liaison
Regulations Analysis
Policy Analysis
Acquisition Reviews
Management Reviews
Office of Current and Emerging Technology Implementation
Federal Information Relay Service
Federal Information Relay Service
Telecomm Customer Requirements
Federal Information Center
Office of GSA-Wide Information Technology D. Vanneberg
Applications Support
Information Resources Management
Automated Office Systems
Liaison
Acquisition & Program Management
Computer Resources Management
Planning & Assurance D. Savoy
Office of Local Telecommunications
Technical Contract Management
Systems Development
National Security/Emergency Preparedness G. Flynn
Resources Management
Systems Management
Office of Information Security T. Burke
Resources Management
Center for Eastern Operations
Center for Eastern Operations
Center for Security Infrastructure Management
Center for Security and Technology Training
Center for Systems Engineering
Center for Business Management
Center for Material and Contract Management

Organization: General Services Administration (GSA)

Senior Information Assurance Official:

Joe M. Thompson, Commissioner, Information Technology Service, GSA

Information Assurance Points of Contact:

Thomas Burke, Deputy Commissioner, Office of Information Security, GSA
G. Flynn, National Security Emergency Preparedness, Office of Local Telecommunications, GSA
R. Woods, Associate Administrator for FTS2000, GSA
D. Venneberg, Deputy Commissioner, Office of GSA-Wide Information Technology, GSA
Diane Savoy, Planning and Assurance Division, Office of GSA-Wide Information Technology, GSA
Bruce Brignall, Post FTS2000 Acquisition Strategy, Office of the Associate Administrator for FTS2000

On-Line Resources:

GSA Homepage: http://www.frbatlanta.org/main/frbsites.htm
GSA Office of Information Security: http://www.gsa.gov/irms/ki/ois.htm
GSA Federal Security Infrastructure: http://www.gsa.gov/fsi/
GSA FSI Civil FORTEZZA Project: http://www.gsa.gov/fsi/fortezza.htm

Information Assurance Related Missions and Functions:

The General Services Administration establishes policy for and provides economical and efficient management of Government property and records, including construction and operation of buildings, procurement and distribution of supplies, utilization and disposal of property; transportation, traffic, and communications management; and management of the Governmentwide automatic data processing resources program. It consists of operating services and support staff offices, with functions carried out at three levels of organization: the central office, regional offices, and field activities.

The Office of Acquisition Policy has a major role in developing, maintaining, issuing, and administering guiding principles via the Federal Acquisition Regulation (FAR) which is applicable to all Federal agencies.

The Office of the Associate Administrator for FTS2000 provides common-user telecommunications and other information services to agencies of the Federal government.

The Information Security Oversight Office is responsible for overseeing executive branch agencies' actions to implement Executive Order 12356, April 2, 1982, which prescribes a uniform system for classifying, declassifying, and safeguarding national security information.

The Office of Information Technology Services provides a variety of services related to information assurance. The office is responsible for coordination and direction of a comprehensive, Government-wide program for the management, procurement, and utilization of automated data processing and local telecommunications equipment and services. The Office of Information Technology Integration provides technical and contracting assistance through three complementary programs: the Federal Systems Integration and Management System (FEDSIM); the Federal Computer Acquisition Center (FEDCAC); and the Federal Information System Support Program (FISSP). The Agency Management Assistance Office conducts several management assistance programs that assist agencies in improving their information-related functions and activities. Among these is the Trail Boss program that helps Federal agencies prepare for major acquisitions. The Information Resources Management Policy Office is responsible for coordinating policy making activities related to information functions and authorities. This office develops, coordinates, and issues Governmentwide automatic data processing and telecommunications acquisition management and use regulations, the Federal Information Resources Management Regulations (FIRMRs). The Information Resources Procurement Office plays a major role in the Governmentwide procurement of automatic data processing and telecommunications hardware, software, and services. In some instances, this office issues a Delegation of Procurement Authority (DPA) which permits Federal agencies to procure their own hardware, software, and services. The Office of Telecommunications Services plays a major role in Governmentwide activities to improve the interagency Information Resources Management (IRM) infrastructure through the Interagency IRM Infrastructure Task Group. This office also manages and administers the National Security Emergency Preparedness Telecommunications Program activities.

Information Assurance Activities, Issues, Best Practices, Lessons Learned:

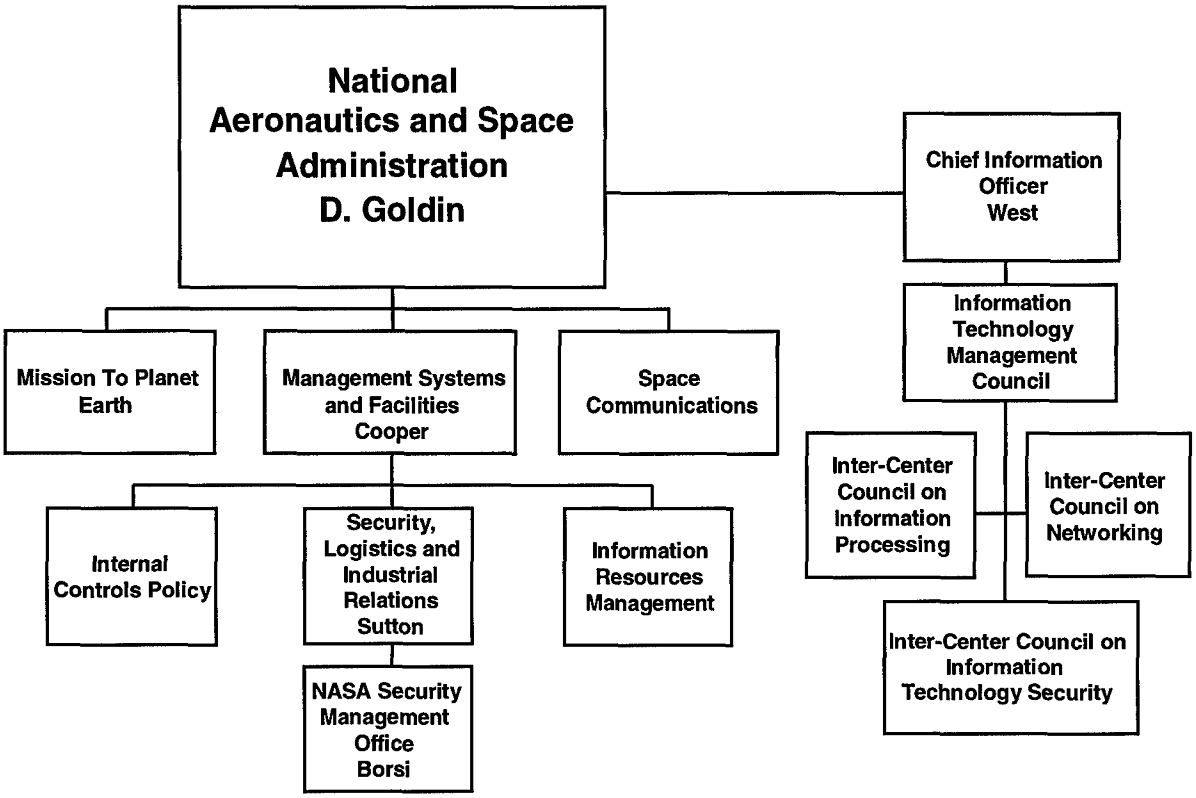
- GSA is involved with infrastructure protection, to include buildings and telecommunications, and works with FEMA and NCS in emergency planning.
- Current objectives are to identify two or three vulnerabilities and to fix them. GSA can not find, fix and react to all security holes, so it must be prudent.
- GSA is planning to encrypt all financial systems in the near future.
- Firewalls and guards are used to protect GSA information and telecommunications and ensure robustness.
- GSA is involved with NSTISSC activities to stand up an infrastructure assurance group, which will coordinate its activities with the Presidential commission.
- A movement towards FORTEZZA is under way that will eventually be implemented in the civil agencies.
- GSA utilizes DOE CERT capabilities for internal assistance. An 800 number has been created that directs calls to the correct incident/emergency response unit.
- Resource reallocation during disruptions of service are managed dynamically by pulled-together teams that draw upon internal assets and expertise.

- GSA released the first draft of a public key encryption policy in April 1996, which is the first step toward establishing government-wide standards for the technology. But the agency must resolve many issues before a final policy can be issued.
- The GSA Office of Information Security was awarded the NSA Rowlett trophy for organizational excellence. GSA's Office of Information Security was recognized for its work in providing technical services to agencies and federal contractors around the globe. The office is also developing security applications for governmentwide electronic commerce and electronic messaging.
- Office of Information Security (OIS) was organized in October 1994, but the services this office provides have been provided by GSA since 1962 beginning with support to the Atomic Energy Commission.
- OIS provides a full spectrum of security services on a reimbursable basis to any customer in the Federal government. The services include engineering, installation, operation and maintenance, systems administration, network management, and a secure packet switching network as a part of FTS 2000. OIS is capable of quick reaction support. The office receives no appropriated moneys. DoD constitutes approximately 60-70 percent of the OIS business and the numbers are growing. Other customers include FBI Legal Attaches, FAA, and the Defense Logistics Agency. These security services support C2, law enforcement operations, regulatory, political, and economic activities, and intelligence operations. OIS also provided coalition warfare support during Desert Shield/Storm and currently supports NATO and UN missions in the Balkans.
- OIS has a long-standing relationship with the National Security Agency (NSA) and the National Institute for Standards and Technology. OIS is currently providing support to the Multilevel Information Systems Security Initiative (MISSI) prototype and to the public key infrastructure prototype. This support includes life-cycle support planning.
- OIS represents GSA in the Information Infrastructure Task Force's (IITF) Security Issues Forum (SIF). OIS participates as a full member in the National Security Telecommunications and Information Systems Security Committee (NSTISSC) and an OIS representative co-chairs, with Treasury, the National Information Infrastructure (NII) Task Force of the NSTISSC. OIS also participates in the Federal Agency Computer Security Program Manager's Forum (FACSPMF). OIS also represents GSA on the Military Communications Electronic Board.
- GSA has three resident program management offices which are chartered by interagency coordinating activities and empowered by agencies and activities having related responsibilities. The offices are the Electronic Commerce Program Management Office (co-chaired by DoD and GSA), the Electronic Mail Program Management Office (chaired by GSA), and the Security Infrastructure Program Management Office which was formed when numerous electronic commerce and electronic mail security issues (such as access control, integrity, non-repudiation, and confidentiality) surfaced. The Electronic Commerce PMO and the Electronic Mail PMO were chartered by the Government Information Technology Services Working Group which supports the Committee on Applications and Technology of the Information Infrastructure Task Force. In addition, the ECPMO was chartered by the Office of Federal Procurement Policy of the Office of Management and Budget. The Security Infrastructure PMO is co-chaired by GSA and

DoD. Intended staffing is approximately 20 people with the staffing being shared among GSA, DISA, NSA, DoJ, Treas, and USPS.

- OIS conducts technical training.
- Issues: Guard technology to allow OIS LAN to interconnect with networks outside the controlled OIS office space.
- Lessons Learned: McAffe network virus checker is identifying viruses other virus checkers should have identified, but did not.
- Information security policy development for GSA is done by the Assurance Division of the Office of GSA-Wide Information Technology. Policy directives in the form of manuals, handbooks, etc. have been published and cover the traditional areas of computer security.
- Brignull operates an interagency group responsible for developing Post FTS2000 acquisition strategy.
- This group is attempting to reach out to the user community to determine needs for Post FTS2000. They have conducted a requirements call and several round tables to address issues such as security and interoperability, wireless services, 800/900 services, data, international, and billing.
- The group seems convinced that there are infrastructure vulnerability problems, but is not sure how to solve them. Possible avenues are legislation, regulation, market forces, and promulgation of industry best practices. Community will also need the help of NIST and NSA.
- The Reliability and Vulnerability Working Group, Telecommunications Policy Committee, Information Infrastructure Task Force, is working on some of the issues. Working group includes has panels working on risk management (chaired by Phil Quaid of NSA), reliability (chaired by Don Nichols of GSA), and standards (chaired by NIST).
- Some of the security and interoperability roundtable issues included warning screens for protected environments, priorities for restoration of services, privacy of billing information, and practicality of standards such as the digital signature standard.
- Of note, cable TV vendors have been added to the FCC's Network Reliability Council and an international subcommittee has also been added to try to collect international outage information. A recommendation has also been made that a security subcommittee be added.
- The Planning and Assurance Division, Office of GSA-Wide Information Technology, is responsible for writing IT systems security policy for GSA internal operations. The Division recently issued policy guidance on use of Internet. It has also recently distributed through electronic mail a policy directive forbidding the downloading of SATAN. Policy directives are issued in the form of GSA Orders, Memos, and IT Program Updates.

This page intentionally left blank.


National Aeronautics and Space Administration D. Goldin
Chief Information Officer West
Information Technology Management Council
Mission To Planet Earth
Management Systems and Facilities Cooper
Space Communications
Inter-Center Council on Information Processing
Inter-Center Council on Networking
Internal Controls Policy
Security, Logistics and Industrial Relations Sutton
Information Resources Management
Inter-Center Council on Information Technology Security
NASA Security Management Office Borsi

Organization: National Aeronautics and Space Administration

Senior Information Assurance Official:

Daniel S. Goldin, Administrator
Ronald S. West, Chief Information Officer
Benita A. Cooper, Associate Administrator for Management Systems and Facilities

Information Assurance Points of Contact:

Russell S. Rice, Director, Information Resources Management Division
Richard W. Carr, NASA Information Technology Security Program Manager
Jeffrey E. Sutton, Director, Security, Logistics, and Industrial Relations Division
Mark J. Borsi, Director, NASA Security Management Office

On-Line Resources:

NASA Homepage: http://www.nasa.gov

Information Assurance Related Missions and Functions:

The National Aeronautics and Space Administration conducts research for the *development of advanced* of problems of flight *designs for aeronautical applications* within and outside the Earth's atmosphere and develops, constructs, tests and operates aeronautical and space vehicles. It conducts activities required for the exploration of space with manned and unmanned vehicles and arranges for the most effective utilization of the scientific and engineering resources of the United States with other nations engaged in aeronautical and space activities for peaceful purposes.

The Office of Mission to Planet Earth conducts NASA's programs that study global climate change and integrated functioning of the Earth as a system. This includes developing and managing remote sensing satellites and instruments, aircraft and ground measurements and research, as well as data and information systems needed to support the objectives of the U.S. Global Change Research Program.

The Office of Space Communications is responsible for meeting requirements critical to NASA's aeronautics and space flight missions. They include spacecraft operations and control centers, ground and space communications, data acquisition and processing, flight dynamics and trajectory analyses, spacecraft tracking and applied research, and development of new technology. A global communications system links tracking sites, control centers, and data processing facilities that provide real-time data processing form mission control, orbit and attitude determination, and routine processing of telemetry data for space missions.

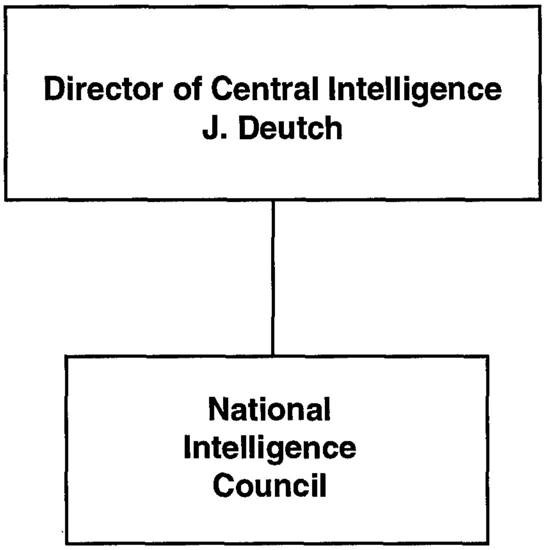
The Goddard Space Flight Center develops and operates information systems technology. The Jet Propulsion Center conducts mission operations and ground based research in information systems technology. The Langley Research Center performs technology experiments in remote sensor and data acquisition and communication technology. The Lewis Research Center conducts research in controls and electronics.

The *NASA CIO* has overall responsibility for information security and information resource management. The NASA Security Management Office is a part of the Security, Logistics and Industrial Relations Division. The Security Management Office is more specifically responsible for policy development and management oversight for *classified information, classified* communications, *classified* automated information, personnel, physical, industrial, and operations security. *Overall corporate-level and Agency-wide functional management* responsibility for Information Technology Security technical integration, implementation, and operation resides in the NASA *CIO* Office.

Information Assurance Activities, Issues, Best Practices, Lessons Learned:

- NASA has an extensive Information Technology Security program that is integrated into its management functions through management points-of-contact, intra-agency working groups, councils, and committees. The goal of the program is to provide cost-effective protection that assures high integrity ready availability, and confidentiality of NASA automated information resources. The program consists of the following basic elements:
  - Policy and guidance
  - Planning
  - Sensitivity and criticality identification
  - Risk management
  - Protection measures baseline
  - Certifications and re-certifications
  - Self-Assessment *and Compliance assurance*
  - Incident response
  - Awareness and training
- Due to NASA's decentralized approach to managing its *diverse and globally connected* computer and network environments, it has adopted a decentralized approach to implementing its ITS program. NASA headquarters interprets national policy and guidance and issues general policy and guidance internally. Each program office is responsible for establishing an information technology security management function which ensures the security, integrity, and continuity of operations for automated information resources directly related to program missions. Each Center and Data Processing Installation is responsible for establishing and sustaining an information technology security program that assures each data processing center under its management complies with security requirements that are consistent with its mission.
- Each Center is responsible for establishing a Computer (and Network) Security Incident Response (CSIR) capability, which is integrated with the Center's Technical Help Desk facility to provide coverage for local computer systems and local area networks. In addition, NASA has an Agency-wide incident response capability (the NASA *Automated Systems* Incident Response Capability (NASIRC)) which has been in existence at the Goddard Space Flight Center for the past *3 1/2* years.

- NASA has instituted a rigorous risk assessment process that includes determining the relative value, sensitivity, and criticality of information, computing, and communications resources. Various protection, detection, and reaction measures are applied to information, communications, and computing resources based on the criticality of various categories of information (e.g., information about persons, mission-critical information) based on the impact loss or destruction of the information or resources might have.
- NASA participates in a variety of interagency information technology security activities to include National Security Telecommunications and Information Systems Security Committee (NSTISSC), the Information Infrastructure Task Force Security Issues Forum (SIF) *Security Policy Board*, Information Systems Security Organization (ISSO), National Institute of Standards and Technology (NIST) Working Groups, and the Forum of Incident Response and Security Teams (FIRST)
- An effective Agency information technology security program must have top-down senior management support and be appropriately placed in the organizational management structure so that it gets the visibility, attention, and resources it needs to get the job done -- and eliminate unnecessary political conflicts of interest.
- An issue of significant importance to NASA is the capability to conduct business electronically. In order to conduct official business (to include typical commerce activities) over the National Information Infrastructure and the Internet, capabilities must exist for effectively and efficiently applying a digital signature *(authentication)* to documents and enclosing those documents in a *secure* envelope *(encryption*) to prevent unauthorized disclosure or manipulation of *official business, scientific, or engineering data/information.*



Director of Central Intelligence
J. Deutch

National
Intelligence
Council

Organization: National Intelligence Council

Senior Information Assurance Official:

Lawrence K. Gershwin, National Intelligence Officer for Science and Technology
MGen John Landry (Ret.), National Intelligence Officer for General Purpose Forces
Mary McCarthy, National Intelligence Officer for Warning

Information Assurance Points of Contact:

Jeffrey Benjamin, Deputy NIO/S&T

On-Line Resources:

Information Assurance Related Missions and Functions:

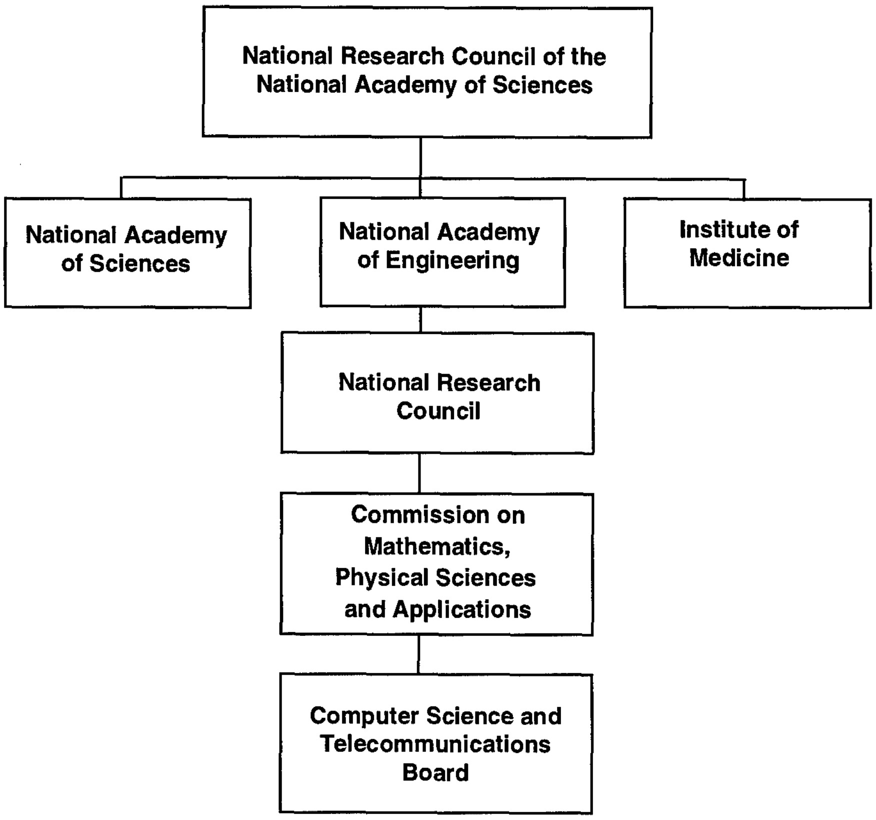
The National Intelligence Council serves as a senior advisory group to the Director of Central Intelligence. National Intelligence Officers (NIOs) support the DCI in his capacity as head of the Intelligence Community by producing interagency reports and analysis, including National Intelligence Estimates.

The NIO for Science and Technology addresses threat issues associated with foreign information warfare plans, programs, and capabilities. Current emphasis is on threats to critical US national-level infrastructures, including the financial sector, electric power distribution, and telecommunications. An Intelligence Community Assessment was completed in 1995, and a more comprehensive NIE on this subject is scheduled for completion by 1 December 1996.

The NIO for General Purpose Forces addresses IW-related threats to US military forces in theater and information-dependent weapon systems.

The NIO for Warning addresses issues associated with indications and warnings for IW. She is sponsoring a DIA-led effort to develop indicators which will help warn of planned or impending IW attacks.

Information Assurance Activities, Issues, Best Practices, Lessons Learned:


National Research Council of the National Academy of Sciences
National Academy of Sciences
National Academy of Engineering
Institute of Medicine
National Research Council
Commission on Mathematics, Physical Sciences and Applications
Computer Science and Telecommunications Board

Organization: National Research Council of the National Academy of Sciences

Senior Information Warfare Official:

Information Warfare Points of Contact:

Marjorie Blumenthal, Director, Computer Science and Telecommunications Board
Herbert Lin, Senior Staff Officer

On-Line Resources:

NRC Homepage: http://www.nas.edu/nrc/

Information Warfare Related Missions and Functions:

The Computer Science and Telecommunications Board (CSTB) is an operating unit within the Commission on Mathematics, Physical Sciences, and Applications of the National Research Council (NRC). The National Research Council is the principal working arm of the National Academy of Sciences, National Academy of Engineering, and the Institute of Medicine--three honorific entities to which distinguished experts in their fields are elected by their peers.

The NRC undertakes work in several major areas of concern: strength of the nation's scientific and technological research and development capabilities; replenishment of scientific and engineering personnel; growth of innovation and productivity; human welfare; education; national security; impact of science and technology on government policy; international scientific and technological relations and competition.

Composed of leaders in the field from industry and academia, the CSTB conducts studies of critical national issues that recommend actions or changes in actions by government, industry, and academic researchers. CSTB also provides a neutral meeting ground for consideration and focusing of complex issues where resolution and action may be premature.

Information Warfare Activities, Issues, Best Practices, Lessons Learned:

- In 1990, the CSTB formed the System Security Study Committee to address the security and trustworthiness of U.S. computing communication systems. The committee was charged with developing a national research, engineering and policy agenda to help the United States achieve a more trustworthy computing technology base by the end of the century. The committee report, *Computers at Risk: Safe Computing in the Information Age*, contains six sets of recommended actions:
  - Promulgating a comprehensive set of generally accepted systems security principles; referred to as GSSP;

- Taking specific short-term actions that build on ready available capabilities;
- Establishing a comprehensive data repository and appropriate education programs to promote public awareness;
- Clarifying export control criteria and procedures;
- Securing funding for a comprehensive, directed program of research; and
- Establishing a new organization to nurture the development, commercialization, and proper use of trust technology, referred to as the Information Security Foundation, or ISF.

- In 1993, the CSTB formed the Committee to Study National Cryptographic Policy. The committee was charged with conducting a comprehensive study of cryptographic technologies and national cryptographic policy. The study assessed the effect of cryptographic technologies on: national security interests of the United States Government; law enforcement interests of the United States Government; commercial interests of United States industry; and privacy interests of United States Citizens. It also assessed the effect of commercial interests of United States industry of export controls on cryptographic technologies.

The committee recently issued its report, "Cryptography's Role in Security the Information Society." The report contained the following recommendations:

A FRAMEWORK FOR NATIONAL CRYPTOGRAPHY POLICY

The framework for national cryptography policy should provide coherent structure and reduce uncertainty for potential vendors and non-government and government users of cryptography in ways that it does not do today. Recommendations 1, 2, and 3 support this basic framework.

Recommendation 1: No law should bar the manufacture, sale, or use of any form of encryption within the United States.

Recommendation 2: National cryptography policy should be developed by the executive and legislative branches on the basis of open public discussion and governed by the rule of law.

Recommendation 3: National cryptography policy affecting the development and use of commercial cryptography should be more closely aligned with market forces.

The committee recognizes that considerations of public safety and national security make it undesirable to maintain an entirely laissez-faire approach to national cryptography policy. But it believes that government intervention in the market should be carefully tailored to specific circumstances. The committee describes a set of appropriate government interventions in Recommendations 4, 5, and 6.

A national cryptography policy that is aligned with market forces would emphasize the freedom of domestic users to determine cryptographic functionality, protection, and implementations according to their security needs as they see fit. Innovation in technologies such as escrowed encryption would be examined by customers for their business fitness of purpose. Diverse user needs would be accommodated; some users will find it useful to adopt some form of escrowed encryption to protect their access to encrypted data, while others will find that the risks of escrowed encryption (e.g., the dangers of compromising sensitive information through a failure of the escrowing system) are not worth the benefits.

Standards are another dimension of national cryptography policy with a significant impact on commercial cryptography and the market. Cryptographic standards that are inconsistent with prevailing or emerging industry practice are likely to encounter significant market resistance. Thus, to the maximum extent possible, national cryptography policy that is more closely aligned with market forces should encourage adoption by the Federal government and private parties of cryptographic standards that are consistent with prevailing industry practice.

Finally, users in the private sector need confidence that products with cryptographic functionality will indeed perform as advertised. To the maximum degree possible, national cryptography policy should support the use of algorithms, product designs, and product implementations that are open to public scrutiny. Information security mechanisms for widespread use that depend on a secret algorithm or a secret implementation invite a loss of public confidence, because they do not allow open testing of the security, they increase the cost of hardware implementations, and they may prevent the use of software implementations as described below. Technical work in cryptography conducted in the open can expose flaws through peer review and assure the private sector user community about the quality and integrity of the work underlying its cryptographic protection.

EXPORT CONTROLS

Recommendation 4: Export controls on cryptography should be progressively relaxed but not eliminated.

Recommendation 4.1: Products providing confidentiality at a level that meets most general commercial requirements should be easily exportable [2].

Recommendation 4.2: Products providing stronger confidentiality should be exportable on an expedited basis to a list of approved companies if the proposed product user is willing to provide access to decrypted information upon legally authorized request.

Recommendation 4.3: The U.S. government should streamline and increase the transparency of the export licensing process for cryptography.

LAW ENFORCEMENT

Recommendation 5: The U.S. government should take steps to assist law enforcement and national security to adjust to new technical realities of the information age.

Recommendation 5.1: The U.S. government should actively encourage the use of cryptography in nonconfidentiality applications such as user authentication and integrity checks.

Recommendation 5.2: The U.S. government should promote the security of the telecommunications networks more actively. At a minimum, the U.S. government should promote the link encryption of cellular communications and the improvement of security at telephone switches.

Recommendation 5.3: To better understand how escrowed encryption might operate, the U.S. government should explore escrowed encryption for its own uses. To address the critical international dimensions of escrowed communications, the U.S. government should work with other nations on this topic.

Recommendation 5.4: Congress should seriously consider legislation that would impose criminal penalties on the use of encrypted communications in interstate commerce with the intent to commit a federal crime.

Recommendation 5.5: High priority should be given to research, development, and deployment of additional technical capabilities for law enforcement and national security to cope with new technological challenges.

PRIVATE SECTOR

Recommendation 6: The U.S. government should develop a mechanism to promote information security in the private sector.

The CSTB has been asked by DARPA to convene a committee that would examine, discuss, and report on interrelated issues relating to research, development, and commercialization of technologies for trustworthy systems. The committee has not been convened at time of publication.

This page intentionally left blank.

Nuclear Regulatory Commission

Organization: United States Nuclear Regulatory Commission (NRC)

Designated Senior Official for Information Resources Management:

Hugh L. Thompson, Jr., Deputy Executive Director for Nuclear Materials Safety, Safeguards, and Operations Support

Information Assurance Points of Contact:

Gerald F. Cranford, Director, Office of Information Resources Management (IRM)
Patricia G. Norry, Director, Office of Administration (ADM)
George H. Messenger, Director, Financial Management, Computer Security and Administrative Support Staff, Office of Information Resources Management (FCAS/IRM)
Raymond J. Brady, Director, Division of Security, Office of Administration, (ADM/SEC)

On-Line Resources:

NRC Homepage: http://www.nrc.gov

Information Assurance Related Missions and Functions:

The mission of the NRC is to ensure that civilian uses of nuclear materials in the United States--in the operation of nuclear power plants and fuel cycle plants, and in medical, industrial, and research applications--are carried out with adequate protection of public health and safety, the environment, and national security.

The NRC accomplishes its purposes by the licensing and regulatory oversight of nuclear reactor operations and other activities involving the possession and use of nuclear materials and wastes; by the safeguarding of nuclear materials and facilities from theft and/or sabotage; by the issuance of rules and standards; and by inspection and enforcement actions.

The NRC was created as an independent agency by the Energy Reorganization Act of 1974, which abolished the Atomic Energy Commission (AEC) and moved the AEC's regulatory function to NRC. This act, along with the Atomic Energy Act of 1954, as amended, provides the foundation for regulation of the nation's commercial nuclear power industry.

The Deputy Executive Director for Nuclear Materials Safety, Safeguards, and Operations Support executes the Executive Director's responsibilities for Nuclear Material Safety and Safeguards (NMSS) programs, including that portion of regional operations dealing with NMSS issues, oversight of enforcement and investigation functions, centralized administrative support services, and centralized information resources management support services.

The Director, Office of Information Resources Management is responsible for the overall direction and management of centralized information resources of the agency in the areas of computer, telecommunications, and information services, including automated systems development and integration, computer operations, database management, data administration, office automation, local and wide area networks, computer and systems security, the Customer Support Center, user training, document control and management, central files, records management, the library, and related technology and information support services to NRC offices.

The Director, Office of Administration is responsible for providing centralized administrative services in the areas of procurement, property management, facilities support, transportation, rulemaking support, Freedom of Information Act requests, publication services, automated graphics, mail and distribution services, local public document rooms, and security.

The Director, Financial Management Computer Security and Administrative Support Staff, Office of Information Resources Management is responsible for managing IRM's financial/administrative support and NRC's computer security program, including reviewing and approving computer security plans; performing risk analyses; providing computer security awareness training; and providing virus protection, eradication and data recovery services.

The Director, Division of Security, Office of Administration, plans, develops, establishes, and administers policies, standards, regulations, and procedures for the overall NRC security program.

Information Assurance Ongoing and Planned Activities:

- Information Security responsibilities are divided in NRC. The Office of Administration is responsible for personnel, facility and information security, including classified information. The Office of Information Resources Management is responsible for unclassified computer and network security.
- A rigorous Information Security Awareness program has just been completed in the agency. A professional video tape was recently developed to allow both Headquarters and Regional managers to efficiently remind employees of the importance of security on information systems.
- The agency is developing a comprehensive Disaster Recovery Plan for Information Systems in the agency.
- The Director IRM serves as Chairman on the National Communications Systems focus team for the National Information Infrastructure.
- The NRC participates in the National Security Telecommunications & Information Systems Security Committee (NSTISSC) as an observer, the National Institute for Standards and Technology (NIST) Federal Computer Security Program Managers' Forum, and the U.S. Security Policy Forum.
- The NRC uses encryption products and restricted access to provide information protection. The agency has conducted penetration studies to determine the robustness of the network security protective mechanisms.

Securities and Exchange Commission
A. Levitt

Organization: Securities and Exchange Commission

Senior Information Assurance Officials:

Information Assurance Points of Contact:

Mike Bartell, Associate Executive Director, SEC Office of Information Technology

On-Line Resources:

SEC Homepage: http://www.sec.gov/

Information Assurance Related Organizations, Missions and Functions:

The SEC is an independent, nonpartisan, quasijudicial regulatory agency with responsibility for administering the federal securities laws. The purpose of these laws is to protect investors in securities markets that operate fairly and ensure that investors have access to disclosure of all material information concerning publicly traded securities. The Commission also regulates firms engaged in the purchase or sale of, people who provide investment advice, and investment companies.

Information Assurance Activities, Issues, Best Practices, Lessons Learned:

- In May 1996, SEC began mandating the electronic filing of annual reports, 10Qs, and other documents by public companies.

U.S. Postal Service

Postmaster General

Marvin Runyon

Organization: United States Postal Service

Senior Information Assurance Officials:

Richard D. Weirich, Vice President, Information Systems

Information Assurance Points of Contact:

Tim Patterson, Program Manager, Telecommunications, ITSC

On-Line Resources:

USPS Homepage: http://www.usps.gov

Information Assurance Related Organizations, Missions and Functions:

The United States Postal Service provides mail processing and delivery to individuals and businesses within the United States. It is also the responsibility of the Postal Service to protect the mails from loss or theft and to apprehend those who violate postal laws.

Information Assurance Activities, Issues, Best Practices, Lessons Learned:

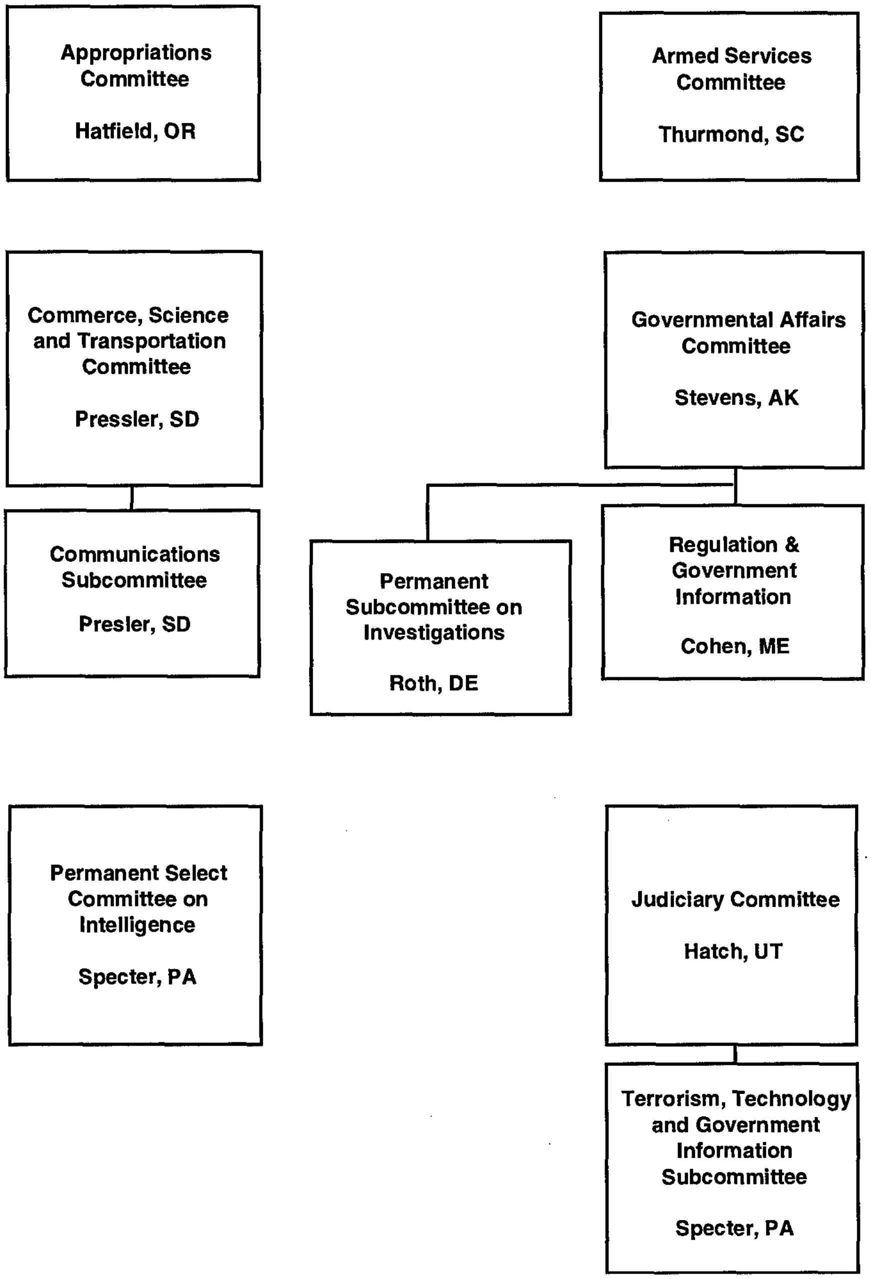
This page intentionally left blank.

Legislative and Judicial

Legislative and Judicial

This page intentionally left blank.

Committees of the Senate



Appropriations Committee

Hatfield, OR

Armed Services Committee

Thurmond, SC

Commerce, Science and Transportation Committee

Pressler, SD

Communications Subcommittee

Presler, SD

Governmental Affairs Committee

Stevens, AK

Permanent Subcommittee on Investigations

Roth, DE

Regulation & Government Information

Cohen, ME

Permanent Select Committee on Intelligence

Specter, PA

Judiciary Committee

Hatch, UT

Terrorism, Technology and Government Information Subcommittee

Specter, PA

Organization: Senate

The bulk of the work of preparing and considering legislation in Congress is done in Committees and Subcommittees. The Committee and Subcommittee and Chairpersons listed below may effect activities. IW relevant charters and focus as well as legislative activity are indicated below. Committees are listed in alphabetical order with associated subcommittees and panels.

On-Line Resources:

Senate Homepage: http://www.senate.gov
Thomas legislative information: http://thomas.loc.gov
Roll Call: http://www.rollcall.com

Committee/Subcommittee: Appropriations Committee

Chairman: Sen. Hatfield, Oregon

Information Assurance Related Missions and Functions:

Information Assurance Activities:

- The Committee is faced with funding the Communications Assistance for Law Enforcement Act of 1994. The act mandated but did not appropriate $500 Million over five years to refund to carriers the cost of modifying their equipment.
- Expected to cut DoC operating budget for telecommunications projects such as the NTIA, NII grants, and Advanced Technology Project.

Committee/Subcommittee: Armed Services Committee

Chairman: Sen. Thurmond, South Carolina

Information Assurance Related Missions and Functions:

Defense budget authorization.

Information Assurance Activities:

Committee/Subcommittee: Committee on Commerce, Science and Transportation

Chairman: Sen. Pressler, South Dakota

Information Assurance Related Missions and Functions:

Information Assurance Activities:

Committee/Subcommittee: Commerce Subcommittee on Communications

Chairman: Sen. Larry Pressler, South Dakota

Information Assurance Related Missions and Functions:

Information Assurance Activities:

Committee/Subcommittee: Governmental Affairs Committee

Chairman: Sen. Stevens, Alaska

Information Assurance Related Missions and Functions:

Privacy Act, regulatory issues, government performance and results

Information Assurance Activities:

Committee/Subcommittee: Governmental Affairs Subcommittee on Regulation and Government Information

Chairman: Sen. Cohen, Maine

Information Assurance Related Missions and Functions:

Information Assurance Activities:

- Sen. Cohen sees information technology as the key to improving Federal government management.

Committee/Subcommittee: Governmental Affairs Permanent Subcommittee on Investigations

Chairman: Roth, DE

Information Assurance Related Missions and Functions:

Information Assurance Activities:

- "Security in Cyberspace" Hearings, May-July 1996

Committee/Subcommittee: Permanent Select Committee on Intelligence

Chairman: Sen. Specter, Pennsylvania

Information Assurance Related Missions and Functions:

Intelligence oversight

Information Assurance Activities:

Committee/Subcommittee: Judiciary Committee

Chairman: Sen. Hatch, Utah

Information Assurance Related Missions and Functions:

Information Assurance Activities:

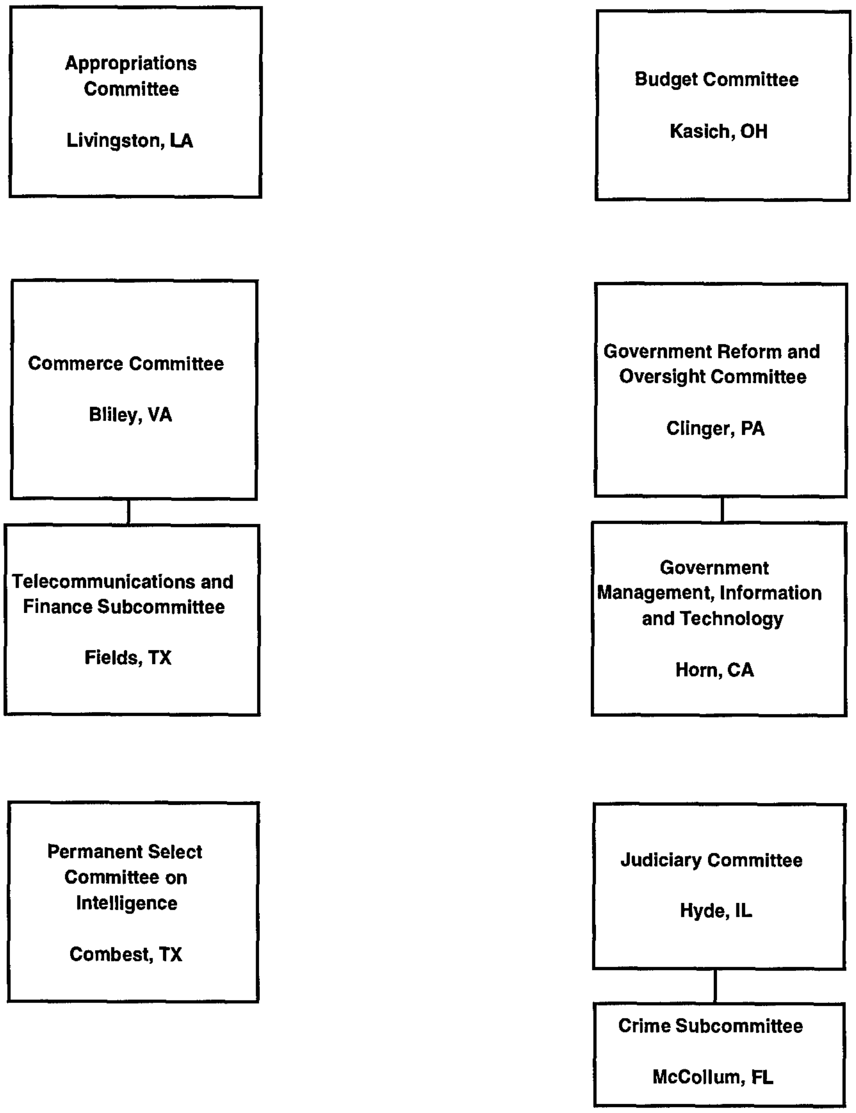
Committee/Subcommittee: Judiciary Subcommittee on Terrorism, Technology and Government Information

Chairman: Sen. Specter, Pennsylvania

Information Assurance Related Missions and Functions:

Information Assurance Activities:

Committees of the House of Representatives



Appropriations Committee

Livingston, LA

Budget Committee

Kasich, OH

Commerce Committee

Bliley, VA

Telecommunications and Finance Subcommittee

Fields, TX

Government Reform and Oversight Committee

Clinger, PA

Government Management, Information and Technology

Horn, CA

Permanent Select Committee on Intelligence

Combest, TX

Judiciary Committee

Hyde, IL

Crime Subcommittee

McCollum, FL

Organization: House of Representatives

The bulk of the work of preparing and considering legislation in Congress is done in Committees and Subcommittees. The Committee and Subcommittee and Chairpersons listed below may affect IW activities. IW relevant charters and focus as well as legislative activity are indicated below. Committees are listed in alphabetical order with associated subcommittees and panels.

On-Line Resources:

House Homepage: http://www.house.gov
Thomas legislative information: http://thomas.loc.gov
Roll Call: http://www.rollcall.com

Committee/Subcommittee: Appropriations Committee

Chairman: Rep. Livingston, Louisiana

Information Assurance Related Missions and Functions:

Budget

Information Assurance Activities:

Committee/Subcommittee: Budget Committee

Chairman: Rep. Kasich, Ohio

Information Assurance Related Missions and Functions:

Budget

Information Assurance Activities:

Committee/Subcommittee: Commerce Committee

Chairman: Rep. Bliley, Virginia

Information Assurance Related Missions and Functions:

Federal Communications Commission

Information Assurance Activities:

Committee/Subcommittee: Commerce Subcommittee on Telecommunications and Finance

Chairman: Rep. Fields, Texas

Information Assurance Related Missions and Functions:

Privacy, telecommunications, finance

Information Assurance Activities:

- Prepared House Telecommunications Reform Bill

Committee/Subcommittee: Government Reform and Oversight Committee (formerly Government Operations Committee)

Chairman: Rep. Clinger, Pennsylvania

Information Assurance Related Missions and Functions:

Civil Service, Postal Service, Washington DC, oversight

Information Assurance Activities:

- Rep. Clinger plans to take the lead role in communicating federal agency information technology needs to the House.
- Rep. Clinger cosponsored the Paperwork Reduction Act.

Committee/Subcommittee: Government Reform and Oversight Subcommittee on Government Management, Information, and Technology (New subcommittee)

Chairman: Rep. Horn, California

Information Assurance Related Missions and Functions:

Privacy Act, NII, paperwork reduction, Federal Agencies

Information Assurance Activities:

Committee/Subcommittee: Permanent Select Committee on Intelligence

Chairman: Rep. Combest, Texas

Information Assurance Related Missions and Functions:

Intelligence oversight

Information Assurance Activities:

Committee/Subcommittee: Judiciary Committee

Chairman: Rep. Hyde, Illinois

Information Assurance Related Missions and Functions:

Information Assurance Activities:

Committee/Subcommittee: Judiciary Subcommittee on Crime

Chairman: Rep. McCollum, Florida

Information Assurance Related Missions and Functions:

FBI, criminal justice

Information Assurance Activities:

Committee/Subcommittee: Committee on National Security (Formerly House Armed Services Committee)

Chairman: Rep. Spence, South Carolina

Information Assurance Related Missions and Functions:

Defense Budget "authorizers"

Information Assurance Activities:

Committee/Subcommittee: Science Committee

Chairman: Rep. Walker, Pennsylvania

Information Assurance Related Missions and Functions:

Information Assurance Activities:

- Rep. Walker is concerned that U.S. standards process is limiting international trade.

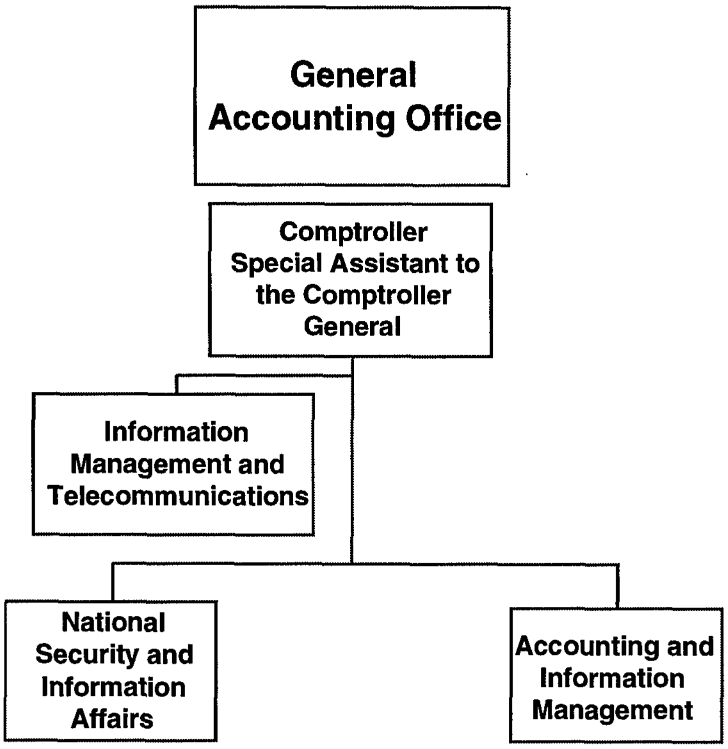
Committee/Subcommittee: Science Subcommittee on Technology

Chairman: Rep Morella, Maryland

Information Assurance Related Missions and Functions:

Information Assurance Activities:

This page intentionally left blank.


General Accounting Office
Comptroller Special Assistant to the Comptroller General
Information Management and Telecommunications
National Security and Information Affairs
Accounting and Information Management

Organization: General Accounting Office (GAO)

Senior Information Assurance Officials:

F. Kevin Boland, Assistant Comptroller General, Office of Information Management and Communications
Jack Brock, Director of Information Resources Management
Butch Hinton, Assistant Comptroller General, National Security and International Affairs Division

Information Assurance Points of Contact:

On-Line Resources:

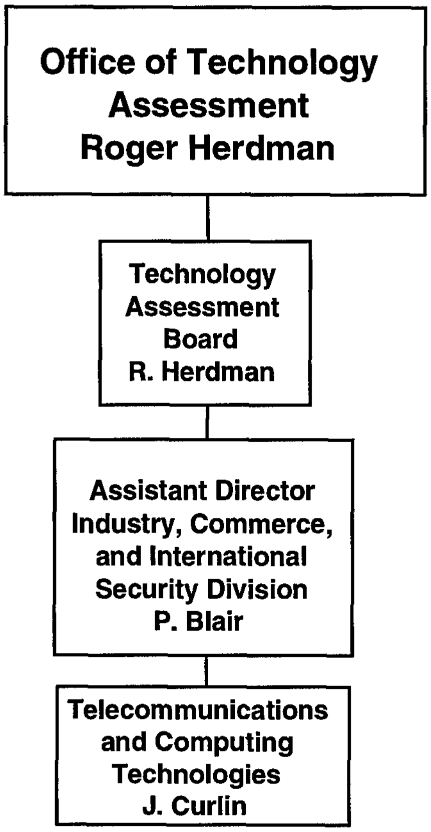
GAO Homepage: http://www.gao.gov

Information Assurance Related Missions and Functions:

The General Accounting Office (GAO) is the audit and investigative arm of the Congress. Its primary function is to respond to requests from Congress for audits and evaluations of government programs and agencies. The GAO also works closely with the Office of Management and Budget and the Secretary of the Treasury to standardize Federal government information systems. The GAO also prescribes accounting standards for the Executive Branch.

Information Assurance Activities, Issues, Best Practices, Lessons Learned:

- GAO continues to find examples of poor information security during audits and investigations.
- Reports issued in 1989, 1991, and 1993 highlight problems with virus' on the Internet, privacy invasions by federal employees, and penetrations of DoD computer systems.
- Internally, GAO has installed Internet connections with firewalls.
- In May 1996, the GAO released a report to Congress entitled *Information Security: Computer Attacks at Department of Defense Pose Increasing Risks* [GAO 1]. On May 22, 1996, GAO testified on their investigation on the first day of hearings on computer security conducted by the Senate Permanent Subcommittee on Investigations, Committee on Governmental Affairs.



Office of Technology Assessment
Roger Herdman

Technology Assessment Board
R. Herdman

Assistant Director
Industry, Commerce, and International Security Division
P. Blair

Telecommunications and Computing Technologies
J. Curlin

Organization: Office of Technology Assessment (OTA)

The OTA was unfunded by Congress in FY 96.

Senior Information Assurance Official:

James Curlin, Program Director, Telecommunications and Computing Technologies

Information Assurance Points of Contact:

On-Line Resources:

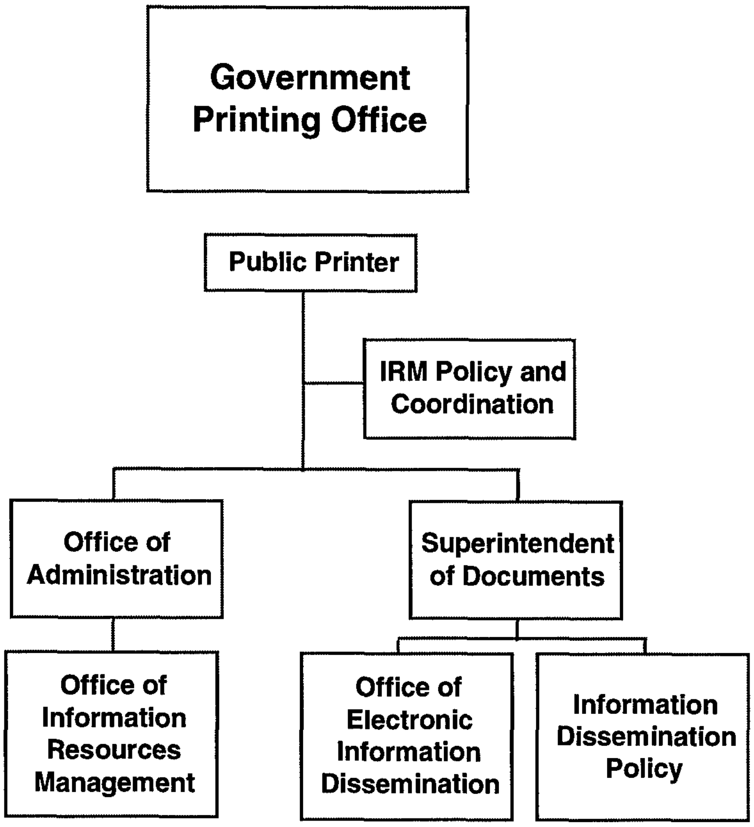
OTA Homepage: http://www.ota.gov

Information Assurance Related Missions and Functions:

The Office of Technology Assessment (OTA) "reports to Congress on the scientific and technical impact of government policies and proposed legislative initiatives." [Office of the Federal Register, 1994] It receives guidance and assignments from a Congressional Board and advice from a Technology Assessment Advisory Council. Its assessments are comprehensive; often taking one to two years to complete, and authoritative as each OTA assessment team is advised by a panel of experts.

Information Assurance Activities, Issues, Best Practices, Lessons Learned:

- OTA reports are comprehensive, authoritative, and readable and are available from the U.S. Government Printing Office.
- In June 1995, OTA published an issue update [OTA 2] of their 1994 report entitled *Information Security and Privacy in Network Environments [OTA 1].* These reports provide useful summaries of the privacy and security background and issues associated with computer networks.


Government Printing Office
Public Printer
IRM Policy and Coordination
Office of Administration
Superintendent of Documents
Office of Information Resources Management
Office of Electronic Information Dissemination
Information Dissemination Policy

Organization: Government Printing Office

Senior Information Assurance Officials:

Patricia R. Gardner, Director of Information Resources Management
Judith Russell, Director of Electronic Information Dissemination Services

Information Assurance Points of Contact:

On-Line Resources:

GPO Homepage: http://www.access.gpo.gov

Information Assurance Related Missions and Functions:

The Government Printing Office (GPO) prints, binds, and distributes documents for the Federal government. It has special statutory authority to make documents available electronically to the public free of charge. It is better known for selling government publications through mail order and GPO bookstores at reasonable prices. It also produces and provides documents on CD-ROM, operates File Transfer Protocol and World Wide Web sites and makes information available through the Federal Bulletin Board.

Information Assurance Activities, Issues, Best Practices, Lessons Learned:

Commission on Protecting and Reducing Government Secrecy

Organization: Commission on Protecting and Reducing Government Secrecy

Senior Information Assurance Official:

Jacques Rondeau, Deputy Staff Director

Information Assurance Point of Contact:

Michael J. White, Senior Professional Staff

On-Line Resources:

Information Assurance Related Missions and Functions:

In examining how to arrive at recommended reforms, the Commission will be guided by the broad interest in careful analysis of the costs -- both qualitative and quantitative --of classification, declassification, and personnel security measures. It also will consider the extent to which there has developed a bureaucratic "culture" generally resistant to change in recent years based on the efforts of senior management at certain agencies as well as outside observers such as the Joint Security Commission. Such an examination will be coupled with a consideration of how best to promote greater "accountability" on the part of those charged with designing and implementing security programs.

Technological innovations present both opportunities and challenges to those responsible for protecting and reducing government secrecy--though many of these consequences only are beginning to be understood within the Federal government and elsewhere.

Information Assurance Activities, Issues, Best Practices, Lesson Learned:

The Impact of Technology on Protecting and Reducing Secrecy

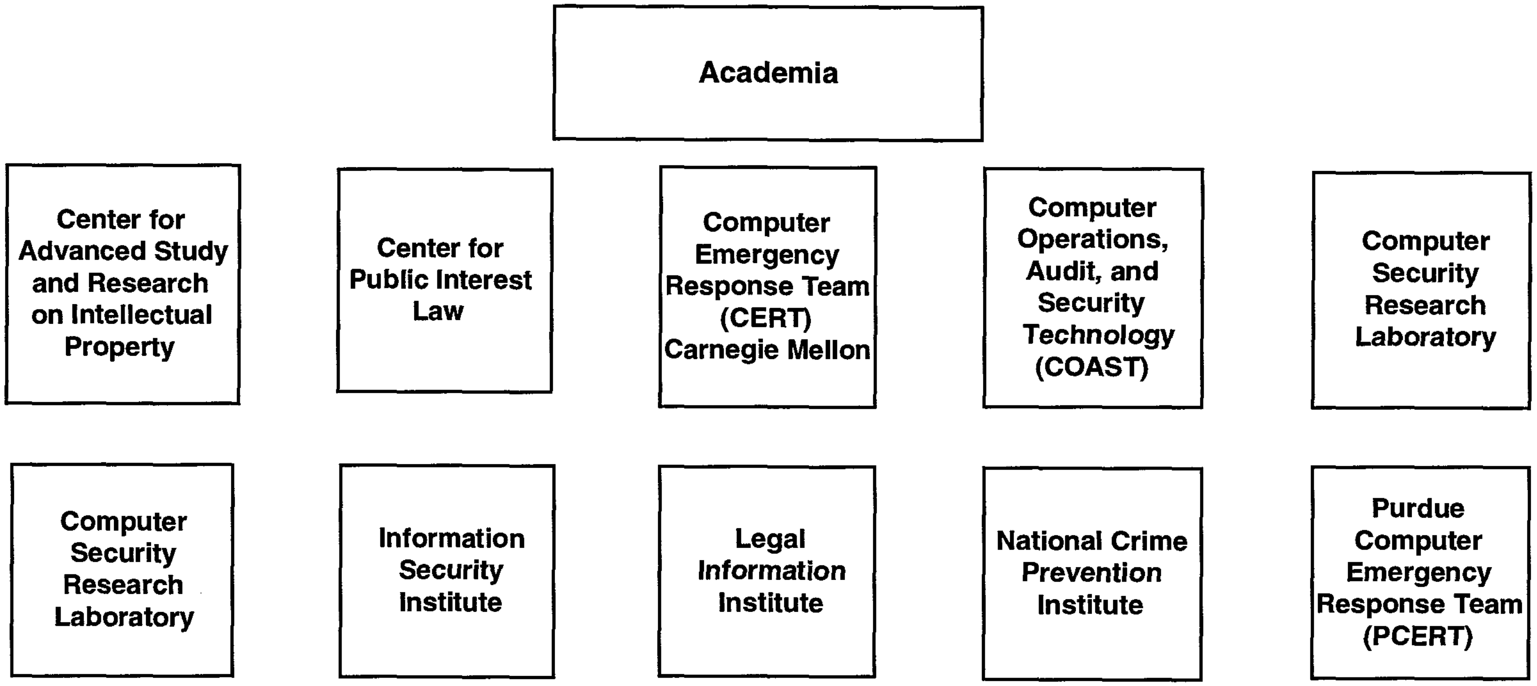
- How is the Government organized to address the effects of technological developments on security policies and procedures?
- How can technology improve public access to information?
- How can technology improve security clearance procedures and the transfer of clearances between agencies?
- How can technology contribute to better protection of classified and sensitive but unclassified information?
- How can technology be used to standardize information systems security?
- How does technology affect the management of security decisionmaking and the formulation of security policies throughout the Government?

This page intentionally left blank.

International, National, State and Local

International, National, State & Local

This page intentionally left blank.



Academia

Center for Advanced Study and Research on Intellectual Property

Center for Public Interest Law

Computer Emergency Response Team (CERT) Carnegie Mellon

Computer Operations, Audit, and Security Technology (COAST)

Computer Security Research Laboratory

Computer Security Research Laboratory

Information Security Institute

Legal Information Institute

National Crime Prevention Institute

Purdue Computer Emergency Response Team (PCERT)

PUBLIC ORGANIZATIONS

ACADEMIA

Center for Advanced Study and Research on Intellectual Property (CASRIP)

University of Washington School of Law, Seattle, WA

URL: http://www.law.washington.edu:80/~casrip/

CASRIP is an independent research and policy development institute focusing on problems in patent and other property ownership rights in the products of high technology. It aims to improve discussion and exchange of views between professionals of various countries, particularly those countries that have major intellectual property systems.

Center for Public Interest Law

University of San Diego School of Law, 5998 Alcala Park, San Diego, CA 92110-2492

URL: http://pwa.acusd.edu/~prc/index.html

This center serves as an academic center of research, learning, and advocacy in administrative law. This center also administers the Privacy Rights Clearinghouse. This Clearinghouse is funded by the Telecommunications Education Trust, a program of the California Public Utilities Commission, and its purpose is to raise consumers' awareness of how technology affects personal privacy.

Computer Emergency Response Team (CERT)

Coordination Center, Software Engineering Institute, Carnegie Mellon University,
Pittsburgh, PA 15213-3890

412/268-7090

Lucy Piccolino, Information Coordinator, 412/268-7700

URL: http://www.sei.cmu.edu/SEI/programs/cert/CERT.info.html

The CERT charter is to work with the Internet community to facilitate its response to computer security events involving Internet hosts, to take proactive steps to raise the community's awareness of computer security issues, and to conduct research targeted at improving the security of existing systems. CERT products and services include a 24-hour technical assistance for responding to computer security incidents, products vulnerability assistance, technical documents, and seminars.

Computer Operations, Audit, and Security Technology (COAST)

Department of Computer Sciences, Purdue University, West Lafayette, IN 47907-1398

URL: http://www.cs.purdue.edu/coast/coast.html

This is a multiple project, multiple investigator effort in computer security research. COAST functions with close ties to researchers and engineers in major companies and government agencies. The focus of their research is on real-world needs and limitations.

Computer Security Research Laboratory

Computer Sciences Department, University of California, 2245 Engineering Unit II,
Davis, CA

916/752-2149

URL: http://seclab.cs.ucdavis.edu/

Research in the Computer Security Research Laboratory is concerned with the development of new techniques for the design of secure systems and for demonstrating such systems to be secure. Current research activities include: (1) developing techniques for understanding malicious code and for detecting and preventing the occurrence of such code in programs, and (2) developing techniques for network intrusion detection. The intent is to flag network intruders and abusers with a low probability of false alarms. The basic philosophy is to employ rule-based approaches to detect policy violations or attempts at exploiting system vulnerabilities. A current project is developing an intrusion detection system that could be used on the INTERNET.

Information Security Institute

George Mason University, Center for Professional Development, 4400 University Drive,
Fairfax, VA 22030-4440

URL: http://www.isse.gmu.edu/~gmuisi/

Legal Information Institute

Cornell Law School, Myron Taylor Hall, Ithaca, NY 14853

URL: http://www.law.cornell.edu/index.html

This institute aims to explore new ways of distributing legal documents and commentary. One primary aim is the dissemination of legal information via the Internet.

National Crime Prevention Institute

University of Louisville, Belknap Campus, Brigman Hall, Louisville, KY 40292

502/852-6987

Wilbur Rykert, Director

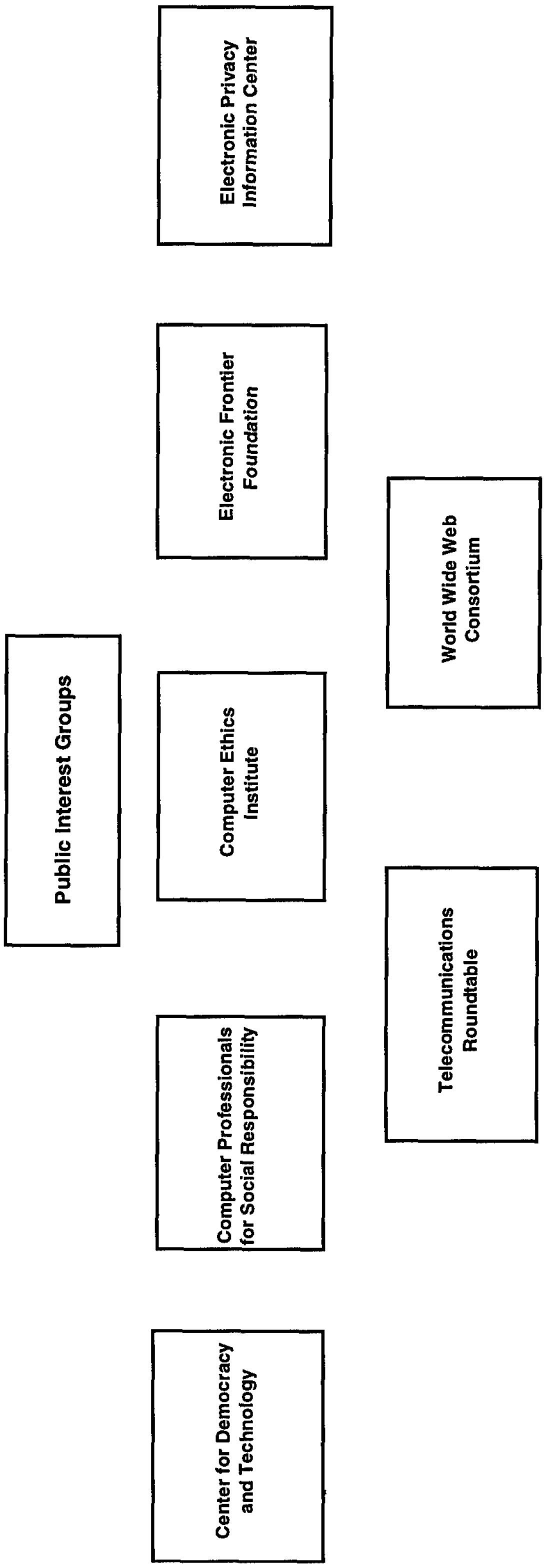
This Institute engages in research pertaining to physical and electronic security and review of loss reduction techniques. The institute trains police officers, criminal justice planners, security personnel in the private sector and community representatives in crime prevention

Purdue Computer Emergency Response Team (PCERT)

Purdue University, Lafayette, Indiana

URL: http://www.cs.purdue.edu/pcert/pcert.html

PCERT is a team of faculty and staff at Purdue University who work together to improve computer security, advise on policies regarding computer use and misuse, and who coordinate responses to computer security incidents on campus. The PCERT is the first university response team admitted to membership in the FIRST.



Public Interest Groups

Center for Democracy and Technology

Computer Professionals for Social Responsibility

Computer Ethics Institute

Electronic Frontier Foundation

Electronic Privacy Information Center

Telecommunications Roundtable

World Wide Web Consortium

PUBLIC ORGANIZATIONS

PUBLIC INTEREST GROUPS

Center for Democracy and Technology

Washington, DC

Jerry Berman

URL: http://www.cdt.org/

This is a non-profit public interest organization; its mission is to develop and advocate public policies that advance constitutional civil liberties and democratic values in new computer and communications technologies. The Center achieves its goals through policy development, public education, and coalition building.

Computer Professionals for Social Responsibility (CPSR)

P.O. Box 717, Palo Alto, CA 94302

415/322-3778

URL: http://snyside.sunnyside.com/home/

This is a non-profit, public interest organization concerned with the effects of computers on society. The mission of CPSR is to provide the public and policymakers with realistic assessments of the power, promise, and problems of information technology.

Electronic Frontier Foundation (EFF)

1550 Bryant Street, Suite 725
San Francisco CA 94117 USA

415 436 9333 (voice)
415 436 9993 (fax)

URL: http://www.eff.org

The EFF is a non-profit, civil liberties, public interest organization founded in July 1990 to ensure that the principles embodied in the Constitution and the Bill of Rights are protected as new communications technologies emerge. The work of this organization focuses on protection of privacy and access to on-line resources and information.

Electronic Privacy Information Center (EPIC)

666 Pennsylvania Avenue, SE, Suite 301, Washington, DC 20003

202/544-9240

Marc Rotenburg, Director
David Sobel, Legal Counsel

URL: http://washofc.epic.org/

This public policy group advocates for electronic privacy. It is a public interest research center, established in 1994 to focus public attention on emerging privacy issues relating to the National Information Infrastructure (NII). It supports efforts to preserve the right of privacy in the electronic age, to give individuals greater control over personal information, and to encourage the development of new technologies that protect privacy rights. It sponsors educational and research programs, a speakers' bureau, compiles statistics, and conducts litigation. It is currently suing the NSC for details on the proposal for NSC to assume oversight of federal information security (see U.S. Security Policy Board).

This page intentionally left blank.

Associations

- American Society for Industrial Security
- Association of Old Crows (Electronic Defense Association)
- Business Espionage Controls and Countermeasures Association
- Communications Fraud Control Association
- Computer Law Association
- Computer Security Institute
- Computer Virus Association
- Data Processing Management Association
- *Forum of Incident* Response and Security Teams
- *High Technology Crime* Investigative Association
- Information Systems Security Association
- International Information Integrity Institute
- Internet Engineering Task Force
- Internet Society
- National Association of Security and Data Vaults
- National Center for Computer Crime Data
- National Classification and Management Society
- National Computer *Security Association*
- Special Interest Group on Operating Systems
- Special Interest Group on Security, Audit and Control
- World Wide Web *Consortium*

PRIVATE ORGANIZATIONS

ASSOCIATIONS

American Society for Industrial Security

1655 North Fort Myer Drive, Suite 1200, Arlington, VA 22209

703/522-5800

Michael Stack, Executive Director; F. Joseph Ricci, Director of Marketing

URL: http://all.net/journal/asis/top.html

This organization acts as a conduit for security professionals; it provides programs and resources at all local, national, and international levels which enable members to update and exchange information and expertise. The role of ASIS Standing Committees and Councils is to keep members informed of the latest developments in security practice and technology and to further integrate specialized knowledge and skills. The ASIS has 27 standing committees, 6 subcommittees, and 3 councils.

- Computer Security Committee: John Spain, Chairman. 404/614-4141.
- Disaster Management Committee: Robert Lee, Chairman. 818/775-4099.
- Government Security Committee: Cynthia Conlon, Chairman. 310/393-0411 X7201.
- Telecommunications Committee: Robert Postovit, Chairman. 206/345-7351.
- Terrorist Activities Committee: Robert Disney, Chairman. 718/481-6400.
- White Collar Crime Committee: Frederick Verinder, Chairman. 202/324-4805.

Association of Old Crows (Formerly the Electronic Defense Association)

1000 N. Payne St., Alexandria, VA 22314

703/549-1600

Gus Slayton, Director

URL: http://www.jedefense.com/jed.html

This is a professional association of scientists, engineers, managers, operators, educators, military personnel and others engaged in the science of electronic warfare and related areas. Approximately 23000 members in 92 regional groups.

Business Espionage Controls and Countermeasures Association

P.O. Box 55582, Seattle, WA 98155

206/364-4672

William Johnson, Executive Director

This association has management consultants, law enforcement officials, and information specialists involved in business espionage controls and countermeasures. Promotes business awareness of the growing concern of espionage in the business community. It publishes "The Business Espionage Report" monthly.

Communications Fraud Control Association

1990 M Street, NW, Suite 508, Washington, DC 20036

202/296-3225

Frances Feld, Executive Director

The thrust of the Association is to find effective ways to combat the growing problem of communications fraud. The Association has the following missions:

- Serves as a clearinghouse for telecommunications fraud information
- Develops training programs on the latest anti-fraud technologies
- Supports legislative protection
- Improve investigative standards and techniques.

Membership includes representatives from MCI, AT&T, SBS, ITT, Network One, many of the Bell Operating Companies and smaller resellers of telecommunications services.

Membership categories include PBX owners, Corporate end-users (Dupont, J.C. Penny, hospitals and universities), International PTTs, Operator Service Providers, Independent Public Payphone Providers, Secret Service and FBI agents, local and Canadian provincial authorities, prosecutors and telecommunication consultants.

Computer Law Association, Inc.

3028 Javier Road, Suite 402, Fairfax, VA 22031
(703) 560-7747 (v) (703) 207-7028 (f)

Founded in 1971, the Computer Law Association has over 1,600 members in thirty-eight countries. The Computer Law Association's non-profit purpose is to inform and educate lawyers about the unique legal issues arising from the evolution, production, marketing, acquisition and use of computer-communications technology. The CLA has sponsored programs and seminars covering a wide-range of topics involving computer law. Such topics include financing, taxation, commercial, contracting, tort liability, and intellectual property rights.

Computer Security Institute

600 Harrison Street, San Francisco, CA 94107

415/905-2370

Patrice Rapalus, Director

URL: http://www.gocsi.com/HomePage.html

Provides computer and information security professionals with information resources and support through membership, training, conferences and networking opportunities. Membership includes many major American Corporations: Aetna Life & Casualty, Allstate Insurance, AT&T, Blue Cross, Boeing Information Services, Chase Manhattan Bank, Coca-Cola Company, Dean Wittier, Dow Chemical, Dupont, Eastman Kodak, Exxon, etc.

Computer Virus Association

408/727-4559

John McAfee, Chairman

This association offers assistance to companies involved in identifying and eradicating computer viruses. It conducts research programs and compiles statistics. Approximately 60 members.

Data Processing Management Association

505 Busse Highway, Park Ridge, IL 60068

708/825-8124

Suzanne Lattimore

URL: http://negaduck.cc.vt.edu/DPMA/

Membership is made up of managerial personnel, staff, educators, and individuals interested in management of information resources. It maintains a Legislative Communications Network, professional education programs, and sponsors student organizations around the country. Membership numbers 24000 in 12 regional groups and 275 local groups.

Forum of Incident Response and Security Teams (FIRST)

National Institute of Standards and Technology, A-216 Technology. Gaithersburg, MD 20899

301/975-3359

URL: http://first.org/first/

FIRST is an international consortium which brings together a variety of computer security incident response teams from government, commercial, and academic organizations. It aims to foster cooperation and coordination in incident prevention, to provide members with technical information, tools, methods, assistance, and guidance, to prompt rapid reaction to incidents, and to promote information sharing among members and the community at large.

High Technology Crime Investigative Association (HTCIA)

P.O. Box 162034, Sacramento, CA 95816

916/441-1333

The HTCIA encourages, promotes, aids and effects the voluntary interchange of data, information, experience, ideas, and knowledge about methods, processes, and techniques relating to investigations and security in advanced technologies among its membership.

Information Systems Security Association, Inc.

800 N. Lingbergh, G2EE, St. Louis, MO 63167

314/694-7661

Ms. Genevieve M. Burns (of Monsanto Corp.), President

URL: http://www.uhsa.uh.edu/issa/

This is an international organization providing educational forums, publications and peer interaction opportunities. The primary goal of ISSA is to promote management practices that will ensure availability, integrity and confidentiality of organizational resources.

Membership: greater than 2,000. Includes major U.S. and international corporations, leading consulting firms, government agencies, and educational institutions. Has more than 35 chapters in major American cities.

International Information Integrity Institute (I4)

333 Ravenswood Avenue, Menlo Park, CA 94025

415/859-4771

Dr. Bruce Baker, Program Manager, SRI International

Assists major enterprises and government agencies in protecting their information assets; I4 is dedicated to advancing information security and enterprise protection by encouraging prudent management responsibilities that lead to a standard of due care.

Internet Engineering Task Force (IETF)

c/o Corporation for National Research Initiatives, 1895 Preston White Drive, Suite 100, Reston, VA

703/620-8990

G. Malkin, IETF Secretariat

URL: http://www.ietf.cnri.reston.va.us/

The IETF is the protocol engineering and development arm of the Internet. It is a large, self-organized, open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet. It is open to any interested individual but there isn't any membership in the IETF. Actual technical work of the IETF is done in its working groups (routing, network management, and security). The mission of the IETF includes: (1) identifying and proposing solutions to pressing operational and technical problems in the Internet, (2) specifying the development or usage of protocols and the near-term architecture to solve such technical problems for the Internet, (3) making recommendations to the Internet Engineering Steering Group (IESG), (4) facilitating technology transfer from the Internet Research Task Force (IRTF) to the wider Internet community, and (5) providing a forum for the exchange of information within the Internet community.

Internet Society

12020 Sunrise Valley Drive, Suite 270, Reston, VA 22091

703/648-9888

Vinton G. Serf, President

URL: http://info.isoc.org/home.html

A nongovernmental, international organization for global cooperation and coordination for the Internet and its technologies and applications. Principal purpose is to maintain and extend the development and availability of the Internet and its associated technologies and applications.

National Association of Security and Data Vaults

716 E. Washington Str., Syracuse, NY 13210

315/475-7743

Ellie Seitz, President

This association has individuals and firms in the private security vault and data storage business. Its accredited members are vault businesses that have met standards set forth by the association. It promotes establishment of non-bank, high-security centers for data storage operations. The association has about 80 members.

National Center for Computer Crime Data

1222 17th Ave., Suite B, Santa Cruz, CA 95062

408/475-4457

Jay J. Bloombecker, Director

This organization is made up of individuals and organizations in the security, law enforcement, legal, business, accounting, and computing professions. It facilitates the prevention, investigation, and prosecution of computer crime by disseminating documents and other data to those in need of such information.

National Classification and Management Society

6118 Roseland Drive, Rockville, MD 20852

301/231-9191

Eugene J. Suto, Executive Secretary

This society manages, supervises, and performs in a security classification management capacity in industry, government, the military services, and educational institutions. The society seeks to establish systems and techniques for identifying information or materials requiring protection in the national interest; it also helps establish procedures and practices for management of classified materials. The society has about 2300 members in 29 local groups.

National Computer Security Association

10 South Courthouse Avenue, Carlisle, PA 17013

717/258-1816

Robert Bales, Executive Officer. Paul Gates, Membership Director

URL: http://www.ncsa.com/

This is a membership organization which provides educational materials, training, testing, and consulting services to improve computer and information security, reliability and ethics.

Special Interest Group on Operating Systems

University of Washington, Department of Computer Sciences, FR-35, Seattle, WA 98195

208/543-9204

Henry Levy, Chairman

URL: http://www.acm.org/sigops/

A special interest group of the Association for Computing Machinery. The group is made up of individuals interested in reliability, integrity and security of data, computer operating systems, communications among computing processes, and much more. Approximately 8100 members.

Special Interest Group on Security, Audit and Control

Association for Computing Machinery, 1515 Broadway, New York, NY 10036

212/869-7440

Daniel Faigin, Chairman

URL: http://www.acm.org/sig_hp/sigsac.html

A special interest group of the Association for Computing Machinery. The groups is made up of information processing security personnel, auditors, accountants and computer technicians. Its purpose is to maintain high levels of skill and awareness regarding technology and practice in the fields of computer security, audit, and control. Approximately 1300 members.

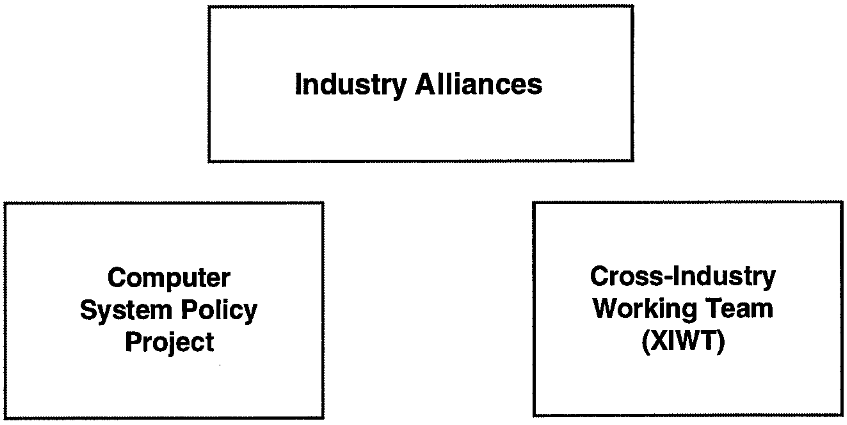
World Wide Web Consortium

Massachusetts Institute of Technology
Laboratory for Computer Science
545 Technology Square
Cambridge, MA 02139

617-253-2613

URL: http://www.w3.org/pub/WWW/

The W3 Consortium exists to develop common standards for the evolution of the World Wide Web. It is an industry consortium run by the Laboratory for Computer Science at the Massachusetts Institute of Technology.



Industry Alliances

Computer System Policy Project

Cross-Industry Working Team (XIWT)

PRIVATE ORGANIZATIONS

INDUSTRY ALLIANCES

Cross-Industry Working Team (XIWT)

c/o Corporation for National Research Initiatives, 1895 Preston White Drive, Suite 100,
Reston, VA, 22091

703/620-8990

Charles N. Brownstein, Executive Director

URL: http://merlin.cnri.reston.va.us:3000/XIWT/

XIWT is a multi-industry coalition committed to defining the architecture and key technical requirements for a powerful and sustainable national information infrastructure (NII). It aims to foster understanding, development and application of technologies that cross industry boundaries, to facilitate the conversion of the NII vision into real-world implementations, and to facilitate a dialogue among representatives of stakeholders in the private and public sectors.

Computer Systems Policy Project

c/o Pam Fandel, Computer System Policy Project, 1735 New York Avenue, NW,
Suite 500, Washington, DC 20006

202/662-8403

URL: http://www.podesta.com/cspp/index.html

The Computer Systems Policy Project (CSPP) is an affiliation of chief executive officers of American computer companies that develop, build, and market information processing systems and software. CSPP's members include the chief executives of Apple, AT&T, Compaq, Control Data Systems, Cray Research, Data General, Digital Equipment, Hewlett-Packard, IBM, Silicon Graphics, Sun Microsystems, Tandem, and Unisys. Upon forming CSPP in 1989, the CEOs made a commitment to work together to develop and personally advocate public policy positions on trade and technology issues that affect their industry, all high-technology industries, and hence, the nation. To date, CSPP has issued numerous reports which outlines the CEO's positions on a variety of issues.

This page intentionally left blank.

Points of Contact

Points of Contact

POINTS OF CONTACT

Three points of contact lists have been provided for the reader's convenience. The first two offer the same information in slightly different formats. The third provides contact information for computer emergency response teams.

- The **Organizational PoC** list is sorted in alphabetical order by organization and by name.
- The **Computer Emergency Response Team** list is sorted in alphabetical order.

Abbreviations have been used in the Organization and Office columns. The following is a list of abbreviations used.

AFIWC	Air Force Information Warfare Center
AIA	Air Intelligence Agency
CDTD	Critical Defense Technology Division
CIA	Central Intelligence Agency
CIAC	Computer Incident Advisory Capability
CISA	C4I Integration Support Activity
CISS	Center for Information Systems Security
CIWE	Center for Information Warfare Excellence
CNA	Center for Naval Analyses
CNO N64	Chief of Naval Operations, Space and Electronic Combat Division
CPRGS	Commission on Protecting and Reducing Government Secrecy
CSIS	Center for Strategic and International Studies
CSSPAB	Computer Systems Security and Privacy Advisory Board
DARPA	Defense Advanced Research Projects Agency
DCI	Director, Central Intelligence
DHHS	Department of Health and Human Services
DIA	Defense Intelligence Agency
DISA	Defense Information Systems Agency
DNA	Defense Nuclear Agency
DoC	Department of Commerce
DoE	Department of Energy
DoI	Department of Interior
DoJ	Department of Justice
DoS	Department of State
DoT	Department of Transportation
DoTreas	Department of the Treasury
DVA	Department of Veterans Affairs
EOP	Executive Office of the President
FACSPMF	Federal Agency Computer Security Program Managers Forum
FBI	Federal Bureau of Investigation
FCC	Federal Communications Commission
FEMA	Federal Emergency Management Agency
FIWC	Fleet Information Warfare Center
FRS	Federal Reserve System
GAO	Government Accounting Office
GPO	Government Printing Office
GSA	General Services Administration
HAC	House Appropriations Committee
HoR	House of Representatives
HQAF	Headquarters, Department of the Air Force
HQDA	Headquarters, Department of the Army
HQMC	Headquarters, Marine Corps
IDA	Institute for Defense Analyses
IIOO	INFOSEC Integration and Oversight Office
IITF	Information Infrastructure Task Force
IRM	Information Resources Management
IWB	Information Warfare Branch
JPSTC	Joint Program Office for Special Technical Countermeasures
JS	Joint Staff
LANL	Los Alamos National Laboratory
LIWA	Land Information Warfare Activity
LIWA	Land Information Warfare Activity
LLNL	Lawrence Livermore National Laboratory
NAS	National Academy of Sciences
NASA	National Aeronautics and Space Administration
NCIS	Naval Criminal Investigative Service
NDU	National Defense University
NEC	National Economic Council
NIMA	National Imagery and Mapping Agency
NIST	National Institute of Standards and Technology
NIWA	Naval Information Warfare Activity
NRC	Nuclear Regulatory Commission
NSA	National Security Agency
NSC	National Security Council
NSTISSC	National Security Telecommunications and Information Systems Security
NTIA	National Telecommunications Information Administration
OASD(C3I)	Office of the Assistant Secretary of Defense (C3I)
ODCSOPS	Office of the Deputy Chief of Staff for Operations and Plans
OGC	Office of the General Council
OIS	Office of Information Security
OMB	Office of Management and Budget
OMNCS	Office of the Manager, National Communications System
ONA	Office of Net Assessment
OoSEC	Office of Security
OSD	Office of the Secretary of Defense
OSI	Office of Special Investigations
OSTP	Office of Science and Technology Policy
OTA	Office of Technology Assessment
OUSD(P)	Office of the Under Secretary of Defense (Policy)
OWTP	Office of Weaponry Technology and Proliferation
PNNL	Pacific Northwest National Laboratory
SAIC	Science Applications International Corporation
SEC	Securities Exchange Commission
SIF	Security Issues Forum

SNL	Sandia National Laboratory
STIC	Science and Technology Information Center
TNSO	Telecommunications and Networking Systems Operation
USA	United States Army
USAF	United States Air Force
USAWC	United States Army War College
USCG	United States Coast Guard
USDA	United States Department of Agriculture
USIA	United States Information Agency
USMC	United States Marine Corps
USN	United States Navy
USPS	United States Postal Service
USSPB	United States Security Policy Board
USSS	United States Secret Service
USSS	United States Secret Service

POINTS OF CONTACT: BY ORGANIZATION

Organization	Office	Name	Phone Number
CIA	OWTP	Chief, CDTD,	703-874-0394
CIA	OWTP	Chief, IWB,	703-874-0281
CNA		Federici, Gary, Mr.	703-824-2504
CPRGS		White, Mike, Mr.	202-776-8753
CSIS		Cilluffo, Frank, Mr.	202-775-3279
CSSPAB		Ware, Willis, Dr.	310-393-0411
DARPA		Lunt, Teresa, Ms.	703-696-4469
DCI		Benjamin, Jeffrey, Mr.	703-482-6811
DCI		Permann, Shelley,	703-482-2381
DHHS		Gignilliat, Bob, Mr.	202-690-7288
DHHS		Taylor, Alford, Mr.	301-443-1167
DHHS		Young, Frank, Dr.	301-443-1167
DIA		Lamb, Mike, Mr.	202-231-4094
DIA		Price, Glenn, Mr.	202-231-3992
DIA		Young, Stan, Mr.	202-373-4500
DIA		Yurechko, John, Mr.	202-373-8384
DISA		Smith, Carl, Mr.	703-607-6759
DISA		Weeks, Rebecca, LtCol	703-607-6096
DISA	CISS	League, Sara Jane, Ms.	703-681-7930
DISA	IIOO	Herrod, Chrisan, Ms.	703-607-6801
DISA	IIOO	Twomey, Tim, Mr.	703-681-7926
DoC		Balutis, Alan, Mr.	202-482-3490
DoC		Gibbon, Jerry, Mr.	202-482-3501
DoC		Hack, Ronald, Mr.	202-482-0120
DoC		Imber, George, Mr.	202-482-0873
DoC		Scott, Tom, Mr.	202-482-0694
DoC		Squier, James, Mr.	202-482-2855
DoC		Zetty, Tom, Mr.	202-482-3501
DoC	NIST	Roback, Ed, Mr.	301-975-3696
DoC	NTIA	Belote, Bill, Mr.	202-482-2473
DoC	NTIA	Gamble, Bill, Mr.	202-482-1850
DoC	NTIA	Parlow, Dick, Mr.	202-482-1850
DoD	JPO STC	Agudo, Mike, Dr.	540-653-6802
DoE		Davis, Mary Beth, Ms.	202-586-5002
DoE		Frampton, Brent, Mr.	202-586-9402
DoE		Przysucha, John, Mr.	301-903-4730
DoE		Rowlett, Tom, Mr.	301-903-3046
DoE		Wallace, Mary Ann, Ms.	301-903-3524
DoE		Wilcher, Larry, Mr.	202-903-5217

Organization	Office	Name	Phone Number
DoE	CIAC	Sparks, Sandra, Ms.	510-422-6856
DoE	LANL	Hunteman, William, Mr.	505-667-0096
DoE	LLNL	Mansur, Doug, Mr.	510-422-0896
DoE	ORNL	Jacobsen, Sharon, Ms.	615-574-0900
DoE	PNNL	Miles, D.R.,	509-372-4515
DoE	SNL	Sprauer, Patricia, Ms.	505-844-1555
DoI		Dolezal, Jim, Mr.	202-208-5002
DoI		Gordon, Gayle, Ms.	202-208-6194
DoJ		Charney, Scott, Mr.	202-514-1026
DoJ		Condon, Mary Ellen, Ms.	202-514-4292
DoJ		Shiveley, Wayne, Mr.	703-827-5110
DoJ		Skolochenko, Steve, Mr.	202-616-1162
DoJ		Stansell-Gamm, Martha, Ms.	202-616-0782
DoJ	FBI	Bryant, Robert, Mr.	202-324-3000
DoJ	FBI	Gallagher, Neil, Mr.	202-324-5740
DoJ	FBI	Geide, Ken, Mr.	202-324-8462
DoJ	FBI	Hughes, Dennis, Mr.	202-234-4974
DoJ	FBI	Perez, Bill, SSA	202-324-5514
DoJ	FBI	Ress, Richard, Mr.	202-324-9168
DoJ	IRM	Boster, Mark, Dr.	202-514-0507
DoS		Geisel, Hal, Mr.	202-647-2889
DoS		Johnson-Braun, Kim, Ms.	202-663-0346
DoS		Lake, Joseph, Mr.	202-647-2889
DoS		McClenaghan, Eliza, Ms.	202-607-2223
DoS		Osthaus, John, Mr.	202-647-2624
DoS		Romagnoli, Jules, Mr.	202-663-0019
DoT		Bussey, III, Jim, LCDR	202-366-9690
DoT		Correia, Nancy, Ms.	202-366-9691
DoT		Kane, Mike, Mr.	202-366-9715
DoT		Taylor, Eugene (Kip), Mr.	202-366-9201
DoT	USCG	Potter, Dave, CAPT	202-267-2766
DoTreas		Chou, Wushow	202-622-1200
DoTreas		Ferris, Marty, Mr.	202-622-2064
DoTreas		Flyzik, Jim, Mr.	202-622-1592
DoTreas		Sullivan, Jane, Ms.	202-622-1599
DoTreas		Wunderlich, Bill, Mr.	202-622-1553
DoTreas	OoSec	Riley, Rick, Mr.	202-622-1120
DoTreas	USSS	Riley, Mary, Ms.	202-435-7823
DoTreas	USSS	Robeck, Mike, Mr.	202-435-5266
DVA		Boyd, Howard, Mr.	202-273-5510
DVA		Lalley, Frank, Mr.	202-565-4311
EOP	NEC	Kalil, Tom, Mr.	202-456-2802

Organization	Office	Name	Phone Number
EOP	NSC	Appel, Ed, Mr.	202-456-9341
EOP	NSC	Beers, Randy, Mr.	202-456-9341
EOP	NSC	Sestak, Joe, CAPT	202-456-9191
EOP	OMB	Brower, Paul, Dr.	202-395-4800
EOP	OMB	McConnell, Bruce, Mr.	202-395-3785
EOP	OMB	Schlarman, Glenn, Mr.	202-395-3785
EOP	OMB	Springer, Ed, Mr.	202-395-3562
EOP	OSTP	Fuhrman, Tom, Mr.	202-456-6057
EOP	OSTP	Johnson, Lee,	202-456-6060
FACSPMF		Pitcher, Sadie, Ms.	202-482-0605
FCC		Kolly, Roy, Mr.	202-418-1150
FCC		Neumann, Herb, Mr.	202-418-2341
FCC		van Doorn, Arlan, Mr.	202-418-1100
FEMA		Donovan, William, Mr.	202-646-3542
FEMA		Green, Dennis, Mr.	202-646-3470
FEMA		Massa, Joe, Mr.	202-646-3083
FRS		Buckley, Ken, Mr.	202-452-3646
FRS		Parrish, John, Mr.	202-452-2224
FRS		Romero, Ray, Mr.	202-452-2832
GAO		Boland, F. Kevin, Mr.	202-512-6623
GAO		Hinton, Buthc, Mr.	202-512-4300
GAO	IRM	Brock, Jack, Mr.	202-512-6240
GPO		Russell, Judith, Ms.	202-512-1265
GSA		Brignall, Bruce, Mr.	703-883-3358
GSA		Flynn, George, Mr.	202-501-0843
GSA		Savoy, Diane, Ms.	202-219-3075
GSA		Venneberg, Don, Mr.	202-501-1000
GSA		Woods, Bob, Mr.	703-285-1020
GSA	OIS	Burke, Tom, Mr.	202-708-7000
GSA	OIS	Specht, John, Mr.	202-708-7000
HoR		Baker, T. Keith, Mr.	703-351-2567
HoR		Haurer, Carroll, Mr.	703-351-2567
HoR		Mullenhoff, Paul, Mr.	703-351-2567
HoR	HAC	Lilly, Scott, Mr.	202-225-3481
IDA		Anthony, Robert, Dr.	703-845-2388
IDA		Barlow, Bill, Mr.	703-845-2465
IDA		Mayfield, Terry, Mr.	703-845-6602
IDA		Shay III, John, Dr.	703-845-2418
IITF		Barrett, Yevette, Ms.	202-482-1835
IITF	SIF	Huth, Virginia, Ms.	202-395-6929
JS		Sharp, Walter, LtCol	703-697-1137
JS	J2	Thompson, Marcum, LtCol	703-614-4921

Organization	Office	Name	Phone Number
JS	J6K	Davis, Kris, LCDR	703-693-4578
JS	J6K	Gorrie, Bob, LTC (P)	703-614-5990
JS	J6K	Gravell, Bill, CAPT	703-614-2918
JS	J6K	Luzwick, Perry, Major	703-697-8896
JS	J6K	Spano, Steve, Lt Col (S)	703-697-1199
JS	J6K	Walsh, Buzz, Major	703-614-2403
JS	NDU	Alger, John, Dr.	202-685-2249
JS	NDU	Barriteau, Brad, Mr.	202-685-2246
JS	NDU	Casey, Richard, Lt. Col.	202-685-2248
JS	NDU	Czerwinski, Tom, Mr.	202-685-2245
JS	NDU	Ducharme, Lee, CDR	202-685-2248
JS	NDU	Giessler, Fred, Dr.	202-685-2258
JS	NDU	Kuehl, Dan, Dr.	202-685-2257
NAS	NRC	Blumenthal, Majorie, Ms.	202-334-2605
NAS	NRC	Lin, Herbert, Mr.	202-334-2605
NASA		Borsi, Mark, Mr.	202-358-0118
NASA		Carr, Rick, Mr.	202-358-2309
NASA		Force, Charles, Mr.	202-358-2020
NASA		Rice, Russel, Mr.	202-358-1790
NASA		Sigust, Art, Mr.	202-358-4787
NASA		Sutton, Jeffrey, Mr.	202-358-2800
NASA		Toraine, Brad, Mr.	301-286-6990
NCIS		Parsons, Mat, SA	202-433-9293
NIST		Grance, Tim, Mr.	301-975-4242
NIST		Katzke, Stuart, Dr.	301-975-2934
NIST		Smid, Miles, Mr.	301-975-2938
NRC		Brady, Raymond, Mr.	301-415-8100
NRC		Cranford, Gerald, Mr.	301-415-7585
NRC		Kellum, Tom, Mr.	301-415-7429
NRC		Kruzic, Pam, Ms.	301-415-7575
NRC		Messenger, George, Mr.	301-415-7546
NRC		Norry, Patricia, Ms.	301-415-7443
NSA		Baggett, Charlie, Mr.	410-684-7087
NSA		Brooks, Clint, Dr.	301-688-4260
NSA		Green, Mike, Mr.	410-859-6884
NSA		Lee, Ronald, Mr.	301-688-6705
NSA		Snow, Brian, Mr.	301-688-8112
NSA		Spencer, John, Mr.	301-688-5131
NSA	CIWE	Larson, Gerald, Mr.	301-688-5131
NSA	NSTISSC	Rothstein, George, Mr.	410-859-6805
OMNCS		Caputo, Chuck, Mr.	703-607-6220
OMNCS		Centra, Mark, Mr.	703-607-6183

Organization	Office	Name	Phone Number
OMNCS		Fletcher, Jim, LTC	703-607-6207
OMNCS		Fountain, Diane, Ms.	703-607-6101
OMNCS	N53	Herr, Fred, Mr.	703-607-6184
OMNCS	N53	Kerr, Jim, Mr.	703-607-6133
OSD	CISA	Miner, Barry, COL	703-695-1081
OSD	OASD(C3I)	Anderson, Bob, Mr.	703-697-5508
OSD	OASD(C3I)	Blackburn, Greg, CAPT	703-693-2157
OSD	OASD(C3I)	Callahan, Roger, Mr.	703-695-8705
OSD	OASD(C3I)	Frizzell, Joe, Dr.	703-697-5508
OSD	OASD(C3I)	Hill, Martin, Mr.	703-614-0624
OSD	OASD(C3I)	O'Neill, Dick, CAPT	703-694-0625
OSD	OASD(C3I)	Soos, James, Dr.	703-695-2396
OSD	OGC	DeRosa, Mary, Ms.	703-695-6710
OSD	ONA	FitzSimonds, Jim, CAPT	703-697-1312
OSD	ONA	Miller, Chuck, COL	703-697-1312
OSD	ONA	Rowell, Scott, COL	703-697-1312
OSD	ONA	van Tol, Jan, CDR	703-697-1312
OSD	OUSD(P)	Dryden, Sheila, Ms.	703-681-9741
OSD	OUSD(P)	Greene, Brent, Mr.	703-614-2616
OSD	OUSD(P)	Guissanie, Gus, Mr.	703-681-5650
OSD	OUSD(P)	Turner, Glenda, Ms.	703-681-5650
SAIC	DoE	Huggin, Ben, Mr.	301-353-8386
SAIC	TNSO	Devost, Matthew, Mr.	703-287-7604
SAIC	TNSO	Hutchins, Rosemary, Ms.	703-734-5832
SAIC	TNSO	Rankin, Bob, Mr.	703-556-7008
SAIC	TNSO	Tompkins, Fred, Mr.	703-821-4385
SAIC	TNSO	Ziegler, Bernie, Mr.	703-790-7452
SEC		Bartell, Mike, Mr.	202-942-8802
SEC		Butler, Wilson, Mr.	202-942-8938
USA	HQDA	Brown, Mike, COL	703-697-1474
USA	HQDA	Harrison, Donal, Mr.	703-697-0612
USA	HQDA	Loranger, Phil, Mr.	703-693-3344
USA	LIWA	Hudson, Tom, LTC	703-706-2263
USA	LIWA	Stevens, Halbert, COL	703-706-1791
USA	LIWA	Virtes, Bob, LTC	703-706-2262
USA	ODCSOPS	Jones, Craig, LTC	703-697-1119
USA	STIC	Burnett, Kay, Ms.	804-980-7884
USA	USAWC	Gooden, R. Thomas, Dr.	717-245-4530
USAF		Bush, Henry, Mr.	315-330-3042
USAF		Goessman, , Mr.	618-256-4450
USAF		Pirog, John, Mr.	315-330-7990
USAF		Rhoades, Walter, Lt Col	803-668-5310

Organization	Office	Name	Phone Number
USAF		Williams, Lee, Capt	617-271-7358
USAF	AFIWC	Ramirez, Fred, Mr.	800-854-0187
USAF	AFIWC	Rodriguez, Feliciano, Mr.	210-977-3990
USAF	AIA	Ramirez, Maria, Ms.	210-977-2465
USAF	HQAF	Blunden, , Lt. Col	703-695-7817
USAF	HQAF	Fiedler, George, Col	703-697-2108
USAF	HQAF	Lieberherr, , Col	703-697-9390
USAF	HQAF	Mullins, Mark, Major	703-697-2108
USAF	HQAF	Wheeler, Greg, Colonel	703-697-8044
USAF	HQAF	Zernial, Ernie, Lt Col	703-697-2108
USAF	OSI	DeMaggio, John, Mr.	202-404-1686
USAF	OSI	Schmidt, Howard, Mr.	202-404-1686
USCG		Chiswell, Ben, CAPT	202-267-6856
USCG		Grimes, Mike, CDR	202-267-1269
USCG		Inman, Mike, LCDR	202-267-6020
USCG		Mead, Mike, CAPT	202-267-2576
USCG		Patrick, Jim, Lt.	202-267-6598
USDA		Boger, Brenda, Ms.	202-720-8025
USDA		Hardesty, Don, Mr.	202-720-3152
USIA		Barnett, Gary, Mr.	202-619-6509
USMC	HQMC	Areola, Dave, CAPT	703-614-4220
USMC	HQMC	Snyder, Marshall, LtCol	703-693-3136
USMC	HQMC	Wiedower, Robert, Major	703-614-4221
USN	CNO N64	Burnette, Gary, LCDR	703-695-0951
USN	CNO N64	Caldarella, Rocco, CAPT	703-695-0951
USN	CNO N64	Galik, D., CDR	703-697-7755
USN	CNON64	Sprout, Rick, Major	703-697-7755
USN	FIWC	Barrett, Gary, CAPT	804-864-8840
USN	NIWA	Handel, Tom, Mr.	301-669-3090
USPS		Patterson, Tim, Mr.	919-501-9074
USSPB		Knauf, Dan, Mr.	703-602-9974
USSPB		LaBarre, Vicki, Ms.	703-602-9993

POINTS OF CONTACT: BY NAME

Name	Organization	Office	Phone Number
Agudo, Mike, Dr.	DoD	JPO STC	540-653-6802
Alger, John, Dr.	JS	NDU	202-685-2249
Anderson, Bob, Mr.	OSD	OASD(C3I)	703-697-5508
Anthony, Robert, Dr.	IDA		703-845-2388
Appel, Ed, Mr.	EOP	NSC	202-456-9341
Areola, Dave, CAPT	USMC	HQMC	703-614-4220
Baggett, Charlie, Mr.	NSA		410-684-7087
Baker, T. Keith, Mr.	HoR		703-351-2567
Balutis, Alan, Mr.	DoC		202-482-3490
Barlow, Bill, Mr.	IDA		703-845-2465
Barnett, Gary, Mr.	USIA		202-619-6509
Barrett, Gary, CAPT	USN	FIWC	804-864-8840
Barrett, Yevette, Ms.	IITF		202-482-1835
Barriteau, Brad, Mr.	JS	NDU	202-685-2246
Bartell, Mike, Mr.	SEC		202-942-8802
Beers, Randy, Mr.	EOP	NSC	202-456-9341
Belote, Bill, Mr.	DoC	NTIA	202-482-2473
Benjamin, Jeffrey, Mr.	DCI		703-482-6811
Blackburn, Greg, CAPT	OSD	OASD(C3I)	703-693-2157
Blumenthal, Majorie, Ms.	NAS	NRC	202-334-2605
Blunden, , Lt. Col	USAF	HQAF	703-695-7817
Boger, Brenda, Ms.	USDA		202-720-8025
Boland, F. Kevin, Mr.	GAO		202-512-6623
Borsi, Mark, Mr.	NASA		202-358-0118
Boster, Mark, Dr.	DoJ	IRM	202-514-0507
Boyd, Howard, Mr.	DVA		202-273-5510
Brady, Raymond, Mr.	NRC		301-415-8100
Brignall, Bruce, Mr.	GSA		703-883-3358
Brock, Jack, Mr.	GAO	IRM	202-512-6240
Brooks, Clint, Dr.	NSA		301-688-4260
Brower, Paul, Dr.	EOP	OMB	202-395-4800
Brown, Mike, COL	USA	HQDA	703-697-1474
Bryant, Robert, Mr.	DoJ	FBI	202-324-3000
Buckley, Ken, Mr.	FRS		202-452-3646
Burke, Tom, Mr.	GSA	OIS	202-708-7000
Burnett, Kay, Ms.	USA	STIC	804-980-7884
Burnette, Gary, LCDR	USN	CNO N64	703-695-0951
Bush, Henry, Mr.	USAF		315-330-3042
Bussey, III, Jim, LCDR	DoT		202-366-9690

Name	Organization	Office	Phone Number
Butler, Wilson, Mr.	SEC		202-942-8938
Caldarella, Rocco, CAPT	USN	CNO N64	703-695-0951
Callahan, Roger, Mr.	OSD	OASD(C3I)	703-695-8705
Caputo, Chuck, Mr.	OMNCS		703-607-6220
Carr, Rick, Mr.	NASA		202-358-2309
Casey, Richard, Lt. Col.	JS	NDU	202-685-2248
Centra, Mark, Mr.	OMNCS		703-607-6183
Charney, Scott, Mr.	DoJ		202-514-1026
Chief, CDTD,	CIA	OWTP	703-874-0394
Chief, IWB,	CIA	OWTP	703-874-0281
Chiswell, Ben, CAPT	USCG		202-267-6856
Chou, Wushow	DoTreas		202-622-1200
Cilluffo, Frank, Mr.	CSIS		202-775-3279
Condon, Mary Ellen, Ms.	DoJ		202-514-4292
Correia, Nancy, Ms.	DoT		202-366-9691
Cranford, Gerald, Mr.	NRC		301-415-7585
Czerwinski, Tom, Mr.	JS	NDU	202-685-2245
Davis, Kris, LCDR	JS	J6K	703-693-4578
Davis, Mary Beth, Ms.	DoE		202-586-5002
DeMaggio, John, Mr.	USAF	OSI	202-404-1686
DeRosa, Mary, Ms.	OSD	OGC	703-695-6710
Devost, Matthew, Mr.	SAIC	TNSO	703-287-7604
Dolezal, Jim, Mr.	DoI		202-208-5002
Donovan, William, Mr.	FEMA		202-646-3542
Dryden, Sheila, Ms.	OSD	OUSD(P)	703-681-9741
Ducharme, Lee, CDR	JS	NDU	202-685-2248
Federici, Gary, Mr.	CNA		703-824-2504
Ferris, Marty, Mr.	DoTreas		202-622-2064
Fiedler, George, Col	USAF	HQAF	703-697-2108
FitzSimonds, Jim, CAPT	OSD	ONA	703-697-1312
Fletcher, Jim, LTC	OMNCS		703-607-6207
Flynn, George, Mr.	GSA		202-501-0843
Flyzik, Jim, Mr.	DoTreas		202-622-1592
Force, Charles, Mr.	NASA		202-358-2020
Fountain, Diane, Ms.	OMNCS		703-607-6101
Frampton, Brent, Mr.	DoE		202-586-9402
Frizzell, Joe, Dr.	OSD	OASD(C3I)	703-697-5508
Fuhrman, Tom, Mr.	EOP	OSTP	202-456-6057
Galik, D., CDR	USN	CNO N64	703-697-7755
Gallagher, Neil, Mr.	DoJ	FBI	202-324-5740
Gamble, Bill, Mr.	DoC	NTIA	202-482-1850
Geide, Ken, Mr.	DoJ	FBI	202-324-8462

Name	Organization	Office	Phone Number
Geisel, Hal, Mr.	DoS		202-647-2889
Gibbon, Jerry, Mr.	DoC		202-482-3501
Giessler, Fred, Dr.	JS	NDU	202-685-2258
Gignilliat, Bob, Mr.	DHHS		202-690-7288
Goessman, , Mr.	USAF		618-256-4450
Gooden, R. Thomas, Dr.	USA	USAWC	717-245-4530
Gordon, Gayle, Ms.	DoI		202-208-6194
Gorrie, Bob, LTC (P)	JS	J6K	703-614-5990
Grance, Tim, Mr.	NIST		301-975-4242
Gravell, Bill, CAPT	JS	J6K	703-614-2918
Green, Dennis, Mr.	FEMA		202-646-3470
Green, Mike, Mr.	NSA		410-859-6884
Greene, Brent, Mr.	OSD	OUSD(P)	703-614-2616
Grimes, Mike, CDR	USCG		202-267-1269
Guissanie, Gus, Mr.	OSD	OUSD(P)	703-681-5650
Hack, Ronald, Mr.	DoC		202-482-0120
Handel, Tom, Mr.	USN	NIWA	301-669-3090
Hardesty, Don, Mr.	USDA		202-720-3152
Harrison, Donal, Mr.	USA	HQDA	703-697-0612
Haurer, Carroll, Mr.	HoR		703-351-2567
Herr, Fred, Mr.	OMNCS	N53	703-607-6184
Herrod, Chrisan, Ms.	DISA	IIOO	703-607-6801
Hill, Martin, Mr.	OSD	OASD(C3I)	703-614-0624
Hinton, Buthc, Mr.	GAO		202-512-4300
Hudson, Tom, LTC	USA	LIWA	703-706-2263
Huggin, Ben, Mr.	SAIC	DoE	301-353-8386
Hughes, Dennis, Mr.	DoJ	FBI	202-234-4974
Hunteman, William, Mr.	DoE	LANL	505-667-0096
Hutchins, Rosemary, Ms.	SAIC	TNSO	703-734-5832
Huth, Virginia, Ms.	IITF	SIF	202-395-6929
Imber, George, Mr.	DoC		202-482-0873
Inman, Mike, LCDR	USCG		202-267-6020
Jacobsen, Sharon, Ms.	DoE	ORNL	615-574-0900
Johnson, Lee,	EOP	OSTP	202-456-6060
Johnson-Braun, Kim, Ms.	DoS		202-663-0346
Jones, Craig, LTC	USA	ODCSOPS	703-697-1119
Kalil, Tom, Mr.	EOP	NEC	202-456-2802
Kane, Mike, Mr.	DoT		202-366-9715
Katzke, Stuart, Dr.	NIST		301-975-2934
Kellum, Tom, Mr.	NRC		301-415-7429
Kerr, Jim, Mr.	OMNCS	N53	703-607-6133
Knauf, Dan, Mr.	USSPB		703-602-9974

Name	Organization	Office	Phone Number
Kolly, Roy, Mr.	FCC		202-418-1150
Kruzic, Pam, Ms.	NRC		301-415-7575
Kuehl, Dan, Dr.	JS	NDU	202-685-2257
LaBarre, Vicki, Ms.	USSPB		703-602-9993
Lake, Joseph, Mr.	DoS		202-647-2889
Lalley, Frank, Mr.	DVA		202-565-4311
Lamb, Mike, Mr.	DIA		202-231-4094
Larson, Gerald, Mr.	NSA	CIWE	301-688-5131
League, Sara Jane, Ms.	DISA	CISS	703-681-7930
Lee, Ronald, Mr.	NSA		301-688-6705
Lieberherr, , Col	USAF	HQAF	703-697-9390
Lilly, Scott, Mr.	HoR	HAC	202-225-3481
Lin, Herbert, Mr.	NAS	NRC	202-334-2605
Loranger, Phil, Mr.	USA	HQDA	703-693-3344
Lunt, Teresa, Ms.	DARPA		703-696-4469
Luzwick, Perry, Major	JS	J6K	703-697-8896
Mansur, Doug, Mr.	DoE	LLNL	510-422-0896
Massa, Joe, Mr.	FEMA		202-646-3083
Mayfield, Terry, Mr.	IDA		703-845-6602
McClenaghan, Eliza, Ms.	DoS		202-607-2223
McConnell, Bruce, Mr.	EOP	OMB	202-395-3785
Mead, Mike, CAPT	USCG		202-267-2576
Messenger, George, Mr.	NRC		301-415-7546
Miles, D.R.,	DoE	PNNL	509-372-4515
Miller, Chuck, COL	OSD	ONA	703-697-1312
Miner, Barry, COL	OSD	CISA	703-695-1081
Mullenhoff, Paul, Mr.	HoR		703-351-2567
Mullins, Mark, Major	USAF	HQAF	703-697-2108
Neumann, Herb, Mr.	FCC		202-418-2341
Norry, Patricia, Ms.	NRC		301-415-7443
O'Neill, Dick, CAPT	OSD	OASD(C3I)	703-694-0625
Osthaus, John, Mr.	DoS		202-647-2624
Parlow, Dick, Mr.	DoC	NTIA	202-482-1850
Parrish, John, Mr.	FRS		202-452-2224
Parsons, Mat, SA	NCIS		202-433-9293
Patrick, Jim, Lt.	USCG		202-267-6598
Patterson, Tim, Mr.	USPS		919-501-9074
Perez, Bill, SSA	DoJ	FBI	202-324-5514
Permann, Shelley,	DCI		703-482-2381
Pirog, John, Mr.	USAF		315-330-7990
Pitcher, Sadie, Ms.	FACSPMF		202-482-0605
Potter, Dave, CAPT	DoT	USCG	202-267-2766

Name	Organization	Office	Phone Number
Price, Glenn, Mr.	DIA		202-231-3992
Przysucha, John, Mr.	DoE		301-903-4730
Ramirez, Fred, Mr.	USAF	AFIWC	800-854-0187
Ramirez, Maria, Ms.	USAF	AIA	210-977-2465
Rankin, Bob, Mr.	SAIC	TNSO	703-556-7008
Ress, Richard, Mr.	DoJ	FBI	202-324-9168
Rhoades, Walter, Lt Col	USAF		803-668-5310
Rice, Russel, Mr.	NASA		202-358-1790
Riley, Mary, Ms.	DoTreas	USSS	202-435-7823
Riley, Rick, Mr.	DoTreas	OoSec	202-622-1120
Roback, Ed, Mr.	DoC	NIST	301-975-3696
Robeck, Mike, Mr.	DoTreas	USSS	202-435-5266
Rodriguez, Feliciano, Mr.	USAF	AFIWC	210-977-3990
Romagnoli, Jules, Mr.	DoS		202-663-0019
Romero, Ray, Mr.	FRS		202-452-2832
Rothstein, George, Mr.	NSA	NSTISSC	410-859-6805
Rowell, Scott, COL	OSD	ONA	703-697-1312
Rowlett, Tom, Mr.	DoE		301-903-3046
Russell, Judith, Ms.	GPO		202-512-1265
Savoy, Diane, Ms.	GSA		202-219-3075
Schlarman, Glenn, Mr.	EOP	OMB	202-395-3785
Schmidt, Howard, Mr.	USAF	OSI	202-404-1686
Scott, Tom, Mr.	DoC		202-482-0694
Sestak, Joe, CAPT	EOP	NSC	202-456-9191
Sharp, Walter, LtCol	JS		703-697-1137
Shay III, John, Dr.	IDA		703-845-2418
Shiveley, Wayne, Mr.	DoJ		703-827-5110
Sigust, Art, Mr.	NASA		202-358-4787
Skolochenko, Steve, Mr.	DoJ		202-616-1162
Smid, Miles, Mr.	NIST		301-975-2938
Smith, Carl, Mr.	DISA		703-607-6759
Snow, Brian, Mr.	NSA		301-688-8112
Snyder, Marshall, LtCol	USMC	HQMC	703-693-3136
Soos, James, Dr.	OSD	OASD(C3I)	703-695-2396
Spano, Steve, Lt Col (S)	JS	J6K	703-697-1199
Sparks, Sandra, Ms.	DoE	CIAC	510-422-6856
Specht, John, Mr.	GSA	OIS	202-708-7000
Spencer, John, Mr.	NSA		301-688-5131
Sprauer, Patricia, Ms.	DoE	SNL	505-844-1555
Springer, Ed, Mr.	EOP	OMB	202-395-3562
Sprout, Rick, Major	USN	CNON64	703-697-7755
Squier, James, Mr.	DoC		202-482-2855

Name	Organization	Office	Phone Number
Stansell-Gamm, Martha, Ms.	DoJ		202-616-0782
Stevens, Halbert, COL	USA	LIWA	703-706-1791
Sullivan, Jane, Ms.	DoTreas		202-622-1599
Sutton, Jeffrey, Mr.	NASA		202-358-2800
Taylor, Alford, Mr.	DHHS		301-443-1167
Taylor, Eugene (Kip), Mr.	DoT		202-366-9201
Thompson, Marcum, LtCol	JS	J2	703-614-4921
Tompkins, Fred, Mr.	SAIC	TNSO	703-821-4385
Toraine, Brad, Mr.	NASA		301-286-6990
Turner, Glenda, Ms.	OSD	OUSD(P)	703-681-5650
Twomey, Tim, Mr.	DISA	IIOO	703-681-7926
van Doorn, Arlan, Mr.	FCC		202-418-1100
van Tol, Jan, CDR	OSD	ONA	703-697-1312
Venneberg, Don, Mr.	GSA		202-501-1000
Virtes, Bob, LTC	USA	LIWA	703-706-2262
Wallace, Mary Ann, Ms.	DoE		301-903-3524
Walsh, Buzz, Major	JS	J6K	703-614-2403
Ware, Willis, Dr.	CSSPAB		310-393-0411
Weeks, Rebecca, LtCol	DISA		703-607-6096
Wheeler, Greg, Colonel	USAF	HQAF	703-697-8044
White, Mike, Mr.	CPRGS		202-776-8753
Wiedower, Robert, Major	USMC	HQMC	703-614-4221
Wilcher, Larry, Mr.	DoE		202-903-5217
Williams, Lee, Capt	USAF		617-271-7358
Woods, Bob, Mr.	GSA		703-285-1020
Wunderlich, Bill, Mr.	DoTreas		202-622-1553
Young, Frank, Dr.	DHHS		301-443-1167
Young, Stan, Mr.	DIA		202-373-4500
Yurechko, John, Mr.	DIA		202-373-8384
Zernial, Ernie, Lt Col	USAF	HQAF	703-697-2108
Zetty, Tom, Mr.	DoC		202-482-3501
Ziegler, Bernie, Mr.	SAIC	TNSO	703-790-7452

COMPUTER EMERGENCY RESPONSE TEAMS

Response Team	Constituency	Email/ WWW URL	Phone #s
Advanced Network Services, INC (ANS)	ANS Customers	anscert@ans.net http://www.ans.net	313-677-7350 313-677-7333 emergency 313-677-7310 fax
Air Force CERT (AFCERT)	Air Force	afcert@afcert.csap.af.mil	210-977-3157 800-854-0187 pager 210-977-4567 fax
Apple Computer	Apple Computer	lsefton@apple.com	408-974-5594 408-974-4754 fax
Australian CERT (AUSCERT)	Australia	auscert@auscert.org.au http://www.auscert.org.au	61-7-3365-4417 61-7-3365-4477
Bellcore	Bellcore	sb3@cc.bellcore.com	908-758-5860 908-758-4504 fax
Boeing CERT (BCERT)	Boeing	compsec@maple.a1.boeing.com	206-657-9405 206-655-2222 emergency 206-657-9477 fax
BSI/GISA	German Government	fwf@bsi.de http://www.cert.dfn.de/eng	49-228-9582-248 49-228-9852-444 emergency 49-228-9582-400 fax
CCTA	UK Government and Agencies	cbaxter.esb.ccta@gnet.gov.uk	44-0171-824-4101/2 44-0171-305-3178 fax
CERT Coordination Center	UNIX, Internet Research	cert@cert.org http://www.cert.org	412-268-7090 412-268-6989 fax
CERT-IT	Italian Internet Sites	cert-it@dsi.unimi.it	39-2-5500-391 39-2-5500-392 emergency 39-2-5500-394 fax
CERT-NL	SURFnet Sites	cert-nl@surfnet.nl http://www.nic.surfnet.nl/surfnet/security/cert-nl.html	31-30-305-305 31-30-305-329 fax
Cisco Systems	Cisco Systems	karyn@cisco.com	408-526-5638 408-526-5420 fax
DEC SSRT	Digital Equipment Corp and Customers	rich.boren@cxo.mts.dec.com	800-354-9000 800-208-7940 emergency 901-761-6792 fax
Defence Research Agency, Malvern	Defense Research Agency	shore@ajax.dra.hmg.gb	44-01684-895425 44-01684-896113 fax
DFN CERT	Germany	dfncert@cert.dfn.de	49-40-54-715-262 49-40-54-715-241 fax
DISA	MILNET	scc@cc.ims.disa.mil	800-365-3642 703-692-5071 fax
DoD ASSIST	DoD Interest Systems	assist@assist.mil	800-357-4231 703-607-4735 fax
DOE CIAC	Department of Energy	ciac@llnl.gov http://ciac.llnl.gov	510-422-8193 510-423-8002 fax
DOW USA	DOW	whstewart@dow.com	517-636-8738 517-638-7705 fax
EDS	EDS and Customers	jcutle01@novell.trts01.eds.com	313-265-7514 313-265-3432 fax

Response Team	Constituency	Email/ WWW URL	Phone #s
FIRST	Forum of Incident Response and Security Teams	first-sec@first.org http://csrc.ncsl.nist.gov/first/	301-975-3359
General Electric	GE Businesses	sandstrom@gies.ges.com	301-340-4848 301-340-4059 fax
Goddard Space Flight Center	Goddard SPC	hmiddleton@gsfcmai.nasa.gov	301-286-7233 301-286-2923 fax
Goldman, Sachs and Company	Goldman, Sachs offices worldwide	safdas@gsco.com	212-357-1880 800-SKY-PAGE (1632254)
Hewlett Packard	All HP-UX Customers	security-alert@hp.com	
Israeli Academic Network	Israeli University users	cert-1@vm.tau.ac.il	972-3-6408309 972-3-6409118 fax
JANET CERT	All JANET networks	cert@cert.ja.net	44-01235-822-302 44-01235-822-898 fax
JP Morgan	JP Morgan employees and consultants		212-235-5010
MCI	Corporate System Security	6722867@mcimail.com	719-535-6932 800-SKY-8888 (190-2130) 719-535-1220 fax
Micro-BIT Virus Center	Anyone	ry15@uni-karlsruhe.de	49-721-376422 49-171-5251685 emergency 49-721-32550 fax
Motorola CERT	Motorola	mcert@mot.com	847-576-1616 847-576-0669 emergency 847-538-2153 fax
NASA (Ames Research Center)	Ames Research Center	hwalter@nas.nasa.gov	415-604-3402 415-604-4377 fax
NASIRC	NASA and International Aerospace community	nasirc@nasirc.nasa.gov http://nasirc.nasa.gov/NASIRC_home.html	800-762-7472 800-SKY-PAGE (2023056) 301-441-1853 fax
NAVCIRT	U.S. Navy	ldrich@fiwc.navy.mil http://infosec.nosc.mil/navcirt.html	804-464-8832 800-SKY-PAGE (5294117)
NIST/CSRC	National Institute of Standards and Tech.	jwack@nist.gov http://cs-www.ncsl.nist.gov	301-975-3359 301-948-0279 fax
NORDUnet	NORDUnet	ber@sunet.se	46-8-790-6513 46-8-24-11-79 fax
Northwestern University	Northwestern Faculty/Staff/Students	r-safian@nwu.edu http://grumpy.acns.nwu.edu/nu-cert	847-491-4056 847-491-3824 fax
Penn State University	Penn State Faculty/Staff/Students	krk5@psu.edu	814-863-9533 814-863-4375 emergency 814-865-3082 fax
Purdue CERT	Purdue University	pcert@cs.purdue.edu http://www.cs.purdue.edu/pcert/pcert.html	317-494-7844 317-494-6440 fax

Response Team	Constituency	Email/ WWW URL	Phone #s
Renater	Minister of Research and Education	morel@urec.fr	33-1-44-27-26-12 33-1-44-27-26-13 fax
SBACERT	Small Businesses Nationwide (US)	hfb@oirm.sba.gov	202-205-6708 202205-7064 fax
Silicon Graphics, Inc	Silicon Graphics User Community	security-alert@sgi.com	415-390-1237 415-390-6236 fax
Stanford University NST	Stanford University Faculty/Staff/Students	security@stanford.edu http://www.stanford.edu/~security/	415-723-2911 415-725-1548 fax
SUN Microsystems	SUN Customers	mark.graff@sun.com	415-786-5274 415-786-7994 fax
SWITCH	Swiss Universities and Government	cert-staff@switch.ch http://www.switch.ch/switch/cert	41-1-268-1518 41-1-760-2137 emergency 41-1-268-1568 fax
TRW Inc.	TRW Network and System Administrators	zorn@gumby.sp.trw.com	310-812-1839 310-813-4621 fax
U.S. Sprint	SprintNet (X.25) and Sprint Link (TCP/IP)	steve.matthews@sprint.sprint.com	703-904-2406 703-904-2708 fax
UCERT	UNISYS Users	garb@po3.bb.unisys.com	215-986-4038 215-330-2316 pager 215-986-4409 fax
Veterans Health Administration IRT	Veteran's Health Administration	frank.marino@forum.va.gov http://www.va.gov	304-263-0811 (4062) 304-263-4748 emergency
Westinghouse Electric Corp.	Westinghouse Corp	nicholson.m%wec@dialcom.tymnet.com	412-642-3097 412-642-3871 fax

This page intentionally left blank.

Appendix B
Reference

Appendix B Reference

U.S. Code

U.S. Code

APPENDIX B

UNITED STATES CODE ANNOTATED BIBLIOGRAPHY AND INDEX

The following is an annotated bibliography of U.S. statutes applicable to Information Warfare and Information Assurance. The abstracts identify the general purpose of the statute and any assigned responsibilities. Key words are also provided. An "Index to Relevant Topics" follows the annotated bibliographies.

Arms Export Control Act of 1968.

KEY WORDS: cryptographic, TEMPEST, export, DoS

ABSTRACT: Export license from the Department of State is required to export cryptographic or TEMPEST information.

Automatic Data Processing Equipment Act of 1965, Public Law 89-306, (Brooks Act) (Repealed in 1996).

KEY WORDS: GSA, Brooks Act, IT procurement, acquisition

ABSTRACT: The Brooks Act amended the Federal Property and Administrative Services Act (FPAS) of 1949. FPAS had previously created the General Services Administration (GSA). The Brooks Act confers upon GSA government-wide responsibility for the economic and efficient acquisition of information technology, including 'sole procurement authority'. In practice, GSA delegates this authority to the agencies. The act implemented a government wide procurement policy promoting competitive bidding, centralized procurement of information technology systems under GSA and established GSA's Board of Contract Appeals. The act assigned responsibilities to the Office of Management and Budget, the Department of Commerce, the National Bureau of Standards (predecessor to National Institute of Standards and Technology) and the General Services Administration for Federal IT procurement. The Paperwork Reduction Act expanded these IT roles. The Computer Security Act specifically assigned information security roles to the Department of Commerce, NIST and GSA and secretaries of Federal departments. With the departure Representative Brooks from Congress, the Brooks Act is a prime target for the 104th Congress as they seek to streamline IT procurement. It is not expected, however, that changes to IT procurement will dramatically change responsibilities for information systems security. The Brooks Act was repealed by the Information Management Reform Act of 1996 (see abstract below).

Cable Communications Policy Act of 1984.

KEY WORDS: cable television, privacy

ABSTRACT: Limits cable television companies in the use of subscriber personal information.

Chief Financial Officers Act of 1990, Public Law 101-576, November 15, 1990.

KEY WORDS: OMB, Federal government, financial management

ABSTRACT: This act enhances the functions of the Office of Management and Budget in order to improve the efficiency and effectiveness of the Federal government. It establishes an Office of Financial Management in OMB and requires a Chief Financial Officer in each Executive agency. Agencies will submit five year financial management plans and status reports and will establish accounting internal controls that provide complete disclosure of agency financial activities.

Communications Act of 1934, Public Law 73-416, June 19, 1934.

KEY WORDS: Commercial carriers, FCC, war powers, NCS

ABSTRACT: Revision of the Radio Act of 1927. The purpose of the Communications Act of 1934 was to regulate interstate and foreign communications by wire and radio in the public interest. It established the Federal Communications Commission and addressed radio stations operated by foreign governments, willful or malicious interference with radio transmissions, and assigned war powers to the President. The Secretary of Commerce will serve as the President's principal adviser on telecommunications policies pertaining to the Nations economic and technological advancement. The Secretary of Commerce will also advise the Director of the Office of Management and Budget relating to the procurement and management of Federal telecommunications systems. The Secretary will also develop policies which relate to international telecommunications issues in coordination with the Secretary of State and other interested agencies. Amendments to the act since 1934 were generally narrow in focus and scope until the Telecommunications Act of 1996 (See Section 2-2, Legal Environment).

Communications Assistance for Law Enforcement Act of 1994, Public Law 103-414, October 25, 1994 (Digital Telephony Act).

KEY WORDS: Intercept, wiretap, carriers

ABSTRACT: The Act required telecommunications carriers to "ensure that its equipment, facilities, or services...are capable of expeditiously isolating and enabling the government, pursuant to a court order or other lawful authorization, to intercept, to the exclusion of other communications, all wire and electronic communications carried by the carrier within a service area to or from equipment [and] to access call-identifying information." Excludes data carriers and on-line services. Network modifications are to be funded by the Federal government, however, funding continues to be a problem. This act also amended the Electronic Communications Act of 1986 to include cordless telephones and certain data communications transmitted over radio. It also clarified fraudulent alteration of commercial mobile radio instruments.

Communications Satellite Act of 1962.

KEY WORDS: FCC, regulatory, satellite

ABSTRACT: This act expanded FCC regulatory jurisdiction assigned by the Communications Act of 1934.

Computer Fraud and Abuse Act of 1986, Public Law 99-474, October 16, 1986.

KEY WORDS: Computer crime, Federal employees, Federal computer systems

ABSTRACT: Made computer fraud or theft across state lines a Federal crime. Also excluded Federal employees from the provisions of Counterfeit Access Device and Computer Fraud and Abuse Act of 1984. It remained a misdemeanor for non-Federal employees to access, use, modify, destroy, or disclose information from a Federal computer. It was feared that Federal employees might be prosecuted for accidental damage or disclosure or whistle blowing.

Computer Matching and Privacy Act of 1988.

KEY WORDS: Privacy, computer matching, Federal government

ABSTRACT: Protects privacy associated with computer matching capabilities and practices of the Federal government. Disclosure and purposes of computer matching are restricted and reporting requirements are levied.

Computer Security Act of 1987, Public Law 100-235, January 8, 1988.

KEY WORDS: NSA, NIST, NSTISSC, CSSPAB, law, sensitive information, classified information, computer security

ABSTRACT: The Computer Security Act assigns responsibilities for the security of sensitive Federal information. NIST is responsible for policy for unclassified-but-sensitive information and is to develop guidance and standards for encryption of data. NIST can, upon request, assist the private sector. NSA is responsible for providing technical assistance to NIST. The act established the National Computer System Security and Privacy Advisory Board (CSSPAB). CSSPAB is a twelve member advisory group of recognized experts in computer and telecommunications systems security and technology. The CSSPAB advises the Secretary of Commerce and Director, NIST. The CSSPAB's mission is to identify issues relative to computer systems security and privacy. The Board focus is limited Federal unclassified systems. The act specifically excludes private sector and Federal classified and Warner Exempt systems. Each Federal agency is to provide mandatory computer security awareness training.

Constitution of the United States, Fourth Amendment, (Bill of Rights), Ratified December 15, 1791.

KEY WORDS: Privacy, unreasonable search, seizure, warrants

ABSTRACT: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."

Counterfeit Access Device and Computer Fraud and Abuse Act of 1984, Public Law 98-473.

KEY WORDS: Computer crime, Federal computers, espionage, computer passwords

ABSTRACT: First computer crime legislation. This statute defined computers, excluding electronic typewriters and hand calculators and addressed the unauthorized access of computer systems making it a felony to access Federal computers to obtain classified information with the intent to do harm to the U.S. or benefit a foreign country. It also made it a misdemeanor to access any Federal computer without authorization. Civil damage suits were authorized against illegal wiretappers. A 1986 amendment made trafficking in stolen computer passwords a criminal act. Under authority of this act, the U.S. Attorney's Office, the FBI and Secret Service engaged in cooperative efforts aimed at computer crime.

Department of Defense Authorization Act of 1982, Public Law 97-86 (Warner Amendment)

KEY WORDS: DoD IT procurement, GSA, Brooks Act, C3I, cryptographic

ABSTRACT: Exempted DoD procurements from the Brooks Act if they involved intelligence, cryptographic, command and control, embedded electronics in a weapon system, or equipment critical to a military or intelligence mission.

Domestic Wiretap Act of 1968 (Federal Wiretap Law).

KEY WORDS: FCC, wiretap, monitoring, consent, e-mail

ABSTRACT: Expanded in 1986 to include computers and electronic mail. Permits monitoring if only one party consents. FCC and some state laws require two-party consent. Violation of FCC regulation is a tariff violation only. Originally FCC required a warning tone but subsequently rescinded that requirement. For government employees, "consent" is more loosely defined. Agency policy and/or stickers on telephone instruments or banners on computer screens during log-on can be considered adequate for "consent."

Electronic Communications Privacy Act of 1986, Public Law 99-508, October 21, 1986.

KEY WORDS: Privacy, wiretap, interception, wire, oral, cellular, cordless, data communications

ABSTRACT: Updated Federal privacy clause in Omnibus Crime Control and Safe Streets Act of 1968 to include digitized voice, data, or video whether transmitted over wire, microwave, or fiber optics. The act applies to transmissions regardless whether they are carried by common or other carriers. Included transmissions where users had an expectation of privacy. Cellular phones were included but cordless were not. The Communications Assistance for Law Enforcement Act of 1994 (Digital Telephony Act) added cordless phones and specified certain data communications transmitted over radio. Warrants are now required for interception of cordless phone conversations. Court warrants, based on probable cause, are required to intercept wire or oral communications. Exceptions to the warrant requirement are: telephone companies and the FCC, police officers when they are a party to the call, and with the consent of one party.

Electronic Funds Transfer Act of 1980.

KEY WORDS: EC/EDI, electronic funds transfer

ABSTRACT: Addresses the privacy of electronic funds transfer. Specifies the responsibilities of financial institutions including a requirement that financial institutions notify customers of the circumstances surrounding third party access to electronic financial information in the course of normal business operations.

Export Administration Act of 1979, Public Law 96-72, September 29, 1979.

KEY WORDS: DoC, export, scientific data, technical data

ABSTRACT: Export of scientific and technical data only authorized with an export license from the Department of Commerce. See also Arms Export Control Act of 1968 for Department of State responsibilities.

Fair Credit Reporting Act of 1970, Public Law 91-508.

KEY WORDS: credit reports, consumer credit

ABSTRACT: Intended to protect the privacy of individuals, the Fair Credit Reporting Act covers consumer credit reports. It details legal uses of credit reports, prohibiting the inclusion of obsolete information and identifies information that must be provided to the U.S. government. It also specifies the process by which a consumer can obtain his credit report and challenge information.

Federal Managers Financial Integrity Act of 1982, Public Law 97-255.

KEY WORDS: Internal controls, NPR, CSSPAB, OMB, GAO, computer security

ABSTRACT: The act amended the Budget and Accounting Act of 1950 to require the GAO to develop internal accounting and administrative standards and OMB to establish guidelines for Executive agencies to conduct annual evaluations of their internal accounting and administrative controls. Annual statements are submitted to the President and Congress. Both the National Performance Review (NPR) and the CSSPAB recommend linking computer security oversight to the oversight required by this act.

Foreign Intelligence Surveillance Act of 1978, Public Law 95-511, October 25, 1978.

KEY WORDS: Foreign intelligence, wiretap, time of war, electronic surveillance, Senate Select Committee on Intelligence

ABSTRACT: The President, through the Attorney General, may, without court order, authorize wiretaps, for up to one year, to gather foreign intelligence subject to certain restrictions. The Attorney General must submit a written oath to a special seven member court established by this act and report minimization procedures to the House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence. The Attorney General may direct communications carriers to support this effort. Other Federal officers must request a court order. Requests must include certifications by the Assistant to the President for National Security Affairs or other executive branch official responsible for national security or defense. During time of war, the President, through the Attorney General, may authorize electronic surveillance without a court order for a period not to exceed fifteen calendar days following a declaration of war by the Congress.

Freedom of Information Acts of 1966 (1969, 1970, 1989), Public Law 93-502.

KEY WORDS: FOIA, national security

ABSTRACT: Companion law to the Privacy Act requiring agencies of the Federal government to release information to citizens. Agencies can refuse to release information related to national security or foreign relations but if challenged in court must prove why the information should not be released.

Government Performance and Results Act of 1993.

KEY WORDS: Strategic planning, performance planning, results

ABSTRACT: Purpose of this act is to systematically hold Federal agencies accountable for achieving program results; improving program effectiveness by focusing on results, service, quality, and customer satisfaction. The act requires Executive agencies, except CIA, USPS, GAO, and others, to draft Strategic Plans no later than September 30, 1997. Special planning and reporting requirements are levied on the USPS. Plans will include relationship between performance goals and general goals and will cover a five year period and be updated every three years. Agencies will also draft annual performance plans covering each program activity in the budget; establishing objective, quantifiable, and measurable performance goals. By March 31, 2000, agencies prepare annual program performance reports; comparing actual performance for against Performance Plans. OMB is the proponent for this act and will identify agencies to participate in pilot projects. OPM will develop manager training. GAO will report to Congress no later than June 1, 1997 on pilot projects and likelihood of other Federal agency compliance.

Information Technology Management Reform Act of 1996, National Defense Authorization Act for Fiscal Year 1996, Public Law 104-106, February 10, 1996

KEY WORDS: Acquisition Reform, IT, Brooks Act

ABSTRACT: The Information Management Reform Act of 1996 is a subordinate act (Division E) of the National Defense Authorization Act for Fiscal Year 1996. The Act repeals the Brooks Automatic Data Processing Act relieving the GSA of responsibility for procurement of automated systems and contract appeals. OMB is charged with providing guidance, policy, and control for information technology procurement. The Act also requires agencies to appoint

Chief Information Officers and to use business process reengineering and performance measures to ensure effective IT procurement and implementation. Changes to Federal Acquisition Regulations, Circular A-130, and a new executive order are expected to help implement the requirements of the Act.

Omnibus Crime Control and Safe Streets Act of 1968, Public Law 90-351.

KEY WORDS: Privacy, wire, oral

ABSTRACT: This act addresses the privacy of wire and oral communications. It specifies the conditions under which an authorized agency may intercept private communications. It was updated by the Electronic Communications Privacy Act of 1986 (P.L. 99-508) in light of new technology.

Paperwork Reduction Act of 1980, Public Law 96-511, December 11, 1980.

KEY WORDS: OMB, IRM, oversight, e-mail, imaging

ABSTRACT: The principal information resources management (IRM) statute for the Federal government. It created the Office of Information and Regulatory Affairs (OIRA) in OMB to establish government-wide IRM policies and oversee and review agency implementation. The act specifically requires agency [sic] to acquire/use IT to improve service delivery and program management, increase productivity, enhance the quality of decision-making, reduce fraud and waste. It also requires that agencies develop a 5-year plan for meeting the agency's IT needs and that the agency head designate a senior IRM official (who reports directly to the agency head) to carry out agency IRM responsibilities under the act. The act also made OMB responsible for improving Federal government administrative efficiency through the use of new technologies such as electronic mail and electronic document storage (imaging). These responsibilities, which complement those in the Communications Act of 1934, give OMB an oversight role in information security. Amended in 1995, the act assigns specific responsibilities for information systems security to OMB, to include oversight of Executive Branch compliance with the Computer Security Act of 1987.

Posse Comitatus Act of 1878, 18 USC 1385, June 18, 1878.

KEY WORDS: Law enforcement, Federal troops

ABSTRACT: The Posse Comitatus Act prohibits the use of the Army and Air Force as posse comitatus. Though not proscribed, the use of the Navy is also generally prohibited by Navy instruction. The Coast Guard is excluded and the Navy may be given permission to assist the Coast Guard. Collaboration of military law enforcement with agents of the Federal, state, and local agencies has generally been found not to violate the act as long as the military role is passive and so long as they never exercise regulatory, proscriptive, or compulsory military in the execution of civilian law enforcement.

Privacy Act of 1974, Public Law 93-579, December 31, 1974.

KEY WORDS: Privacy, access, civil damages, security

ABSTRACT: The objective of the Privacy Act of 1974 is to protect personal privacy from invasions by Federal agencies, in light of increasing use of information technology in the Federal government and the associated increase in personal information maintained by Federal agencies. The law allows individuals to specify what information may be held by a government agency and gives individuals the right to obtain information held on them by the Federal government. The act specifies physical security practices, information management practices, and computer and network controls necessary to ensure individual privacy. It also levied civil and criminal penalties for violations of the provisions of the act.

Right to Financial Privacy Act of 1978

KEY WORDS: Privacy, financial, investigators

ABSTRACT: The Financial Privacy Act requires investigators to present "formal written requests" to review the financial records on an individual held by a financial institution. Investigators must simultaneously notify the individual.

Semiconductor Chip Protection Act of 1984, Public Law 98-620, November 8, 1984.

KEY WORDS: Intellectual property, copyright, computer chips, mask work

ABSTRACT: This act extends copyright protection for 10 years to the owner/creator of the mask work contained in a semiconductor chip. Protection extends from the day the work is registered or commercially exploited anywhere in the world. The President, by proclamation, extend equal protection to foreign nationals if the nation recognizes equal protection to U.S. nationals.

Violent Crime Control and Law Enforcement Act of 1994, Public Law 103-322, September 13, 1994 (Crime Bill of 1994; Computer Abuse Amendments Act of 1994).

KEY WORDS: Computer Fraud and Abuse Act, financial systems, Federal computer laws

ABSTRACT: Section 29000 of this act is cited as the Computer Abuse Amendments Act of 1994. This act changes Federal computer crime to specifically define illegal activity on computers used in interstate commerce or communications. It also treats damage by unauthorized and authorized--insiders vs. trespassers--equally. Through an oversight, the act deleted language in the Computer Fraud and Abuse Act of 1986 which protected Federal and financial computer systems from unauthorized access, alteration or damage. The 104th Congress is expected to correct this oversight. Both acts exclude computers used in foreign commerce. The act also makes intentional damage of a computer system or information a felony but accidental or reckless damage remains a misdemeanor. Some in the information warfare community view this as a decriminalization of hacking.

U.S. CODE
INDEX TO RELEVANT TOPICS

Title	Section	Description
5	552	**Privacy Act of 1974**
5	552	Access to and disclosure of ADP records on individuals
5	552	**Freedom of Information Act of 1966, 1969, 1970, 1989**
5	552	Federal agencies may not sell or rent mailing lists
8	1182	Any foreigner may request a list from the INS automated listing of undesirable visitors. DoS and DoJ must publish guidelines for updating list.
10	2315	National security systems
12	3401	**Right to Financial Privacy Act of 1978**
15	271-278	**National Bureau of Standards Act of 1901**
15	1052	Trademark registration (Lanham Act)
15	1681	**Fair Credit Reporting Act of 1970**
15	1693	**Electronic Funds Transfer Act of 1980**
15	1802	Carriers furnishing information necessary to accomplish electronic surveillance
18	105	Sabotage
18	644	Embezzlement of public money by bank employees
18	793	Gathering information about U.S. communications facilities or defense information for a foreign power
18	1029	**Credit Card Fraud Act**
18	1029	Fraudulent use of credit cards, passwords, or telephone access codes
18	1030	**Counterfeit Access Device and Computer Fraud and Abuse Act, 1984**
18	1030	**Computer Fraud and Abuse Act of 1986**
18	1343	Wire fraud using interstate communications systems
18	1362	Civil defense functions of U.S., malicious injury to government property
18	1385	**Posse Comitatus Act of 1878**
18	2071	Concealment, removal or mutilation of public records
18	2319	Criminal infringement of copyright
18	2510	**Electronic Communications Privacy Act of 1986**
18	2510	**Omnibus Crime Control and Safe Streets Act of 1968**
18	2510	Interception of wire, oral, or electronic communications
18	2510	Electronic communications, defined
18	2510	Electronic storage, defined
18	2510	Oral communications, defined
18	2510	Wire communications, defined
18	2511	Intentional interception and disclosure of content, criminal
18	2511	Electronic surveillance of foreign intelligence by U.S. government, limitations
18	2511	Radio interceptions; permissible

Title	Section	Description
18	2511	Authorization for electronic surveillance to determine existence and capability of equipment of non-authorized persons; excepted conduct
18	2511	Consent to COMSEC monitoring
18	2512	Prohibitions against assembly of electronic intercept devices
18	2512	Contract for manufacturing or distribution of intercepting devices
18	2516	Interception of Wire, Oral, or Electronic communications
18	2516	**Atomic Energy Act of 1954**
18	2516	Interception of currency transactions
18	2516	Military assistance and sales; arms exports
18	2517	Privileged communications
18	2518	Emergency interception; application
18	2701	Unauthorized access to electronic information
18	2702	Stored wire and electronic communications and transactional records access; disclosure of contents
18	2703	Stored wire and electronic communications and transactional records access; Government access
18	2709	Stored wire and electronic communications and transactional records access; Foreign powers
18	2710	Stored wire and electronic communications and transactional records access; definitions
18	2778	Export of software or data controlled by DoD
19	482	Customs officers may stop/search with reasonable cause merchandise was imported against law or w/o paying duty tax
22	2751 et seq.	**Arms Export Control Act of 1968**
22	2751 et seq.	Export of cryptographic and TEMPEST information
26	408	Social security numbers
26	6103	Tax Records
29	2001	**Employee Polygraph Protection Act of 1988**
31	3512	**Chief Financial Officers Act**
31	3512	**Federal Managers Financial Integrity Act**
35	181 et seq.	**Invention Secrecy Act of 1951**
40	759	**Computer Security Act of 1987** (See also National Bureau of Standards Act; 15 USC 271)
40	759	Information systems defined
42	653	Dept. of Health and Hum Services is authorized to match welfare rolls with payroll lists to identify fraudulent welfare claims.
42	2000	**Privacy Protection Act of 1980**
42	2000	Privacy; unlawful acts
42	2011 et	**Atomic Energy Act of 1954**

Title	Section	Description
	seq.	
44	3501	**Paperwork Reduction Act of 1980**
44	3501	**Paperwork Reduction Act of 1995**
44	3501	OMB responsibility to provide overall direction in development and regulation of Federal information policies. Monitor compliance with Privacy Act .
45	83	Continuous lines, railroad and telegraph
47	13	Violations of laws, civil and criminal liability of carriers
47	151 et seq.	**Communications Act of 1934**
47	151 et seq.	**Telecommunications Act of 1996**
47	152	Applicability of Communications Act of 1934 to cable television
47	154	Cooperation and coordination of radio and wire communications, investigations
47	227	**Automated Telephone Consumer Protection Act of 1991**
47	305	Office of Science and Technology, war powers functions of President assigned to (See also Executive Order 12046
47	305	Telecommunications advisory committees, establishment, composition (See also Executive Order Number 12046)
47	305	Construction and operation of foreign government radio station in U.S. (See also Exec Order Number 12046)
47	305	Presentation of Executive Branch views to, functions of Secretary of Commerce
		Disclosure of information
47	305	Coordination functions of Secretary of Commerce concerning telecommunications
47	305	Telecommunications functions assigned to Secretary of Commerce
47	305	Functions assigned to OMB
47	305	Functions assigned to NSC and OSTP
47	305	Functions assigned to Department of State
47	551	Disclosure of information, protection of cable television subscriber privacy
47	605	Unauthorized use or publication of communications
47	605	Need for encryption standard in cable television
47	605	Unauthorized use or publication of communications
47	605	Foreign intelligence gathering
47	605	Blue boxes
47	605	Mobile telephone
47	605	Consent to COMSEC monitoring
47	606	Powers of President during War
47	606	Obstruction of interstate or foreign communications during War
47	609	**Federal Communications Commission Authorization Acts of 1983, 1988,**

Title	Section	Description
		1990
47	701-744	**Communications Satellite Act of 1962**
47	701	Communications Satellite System
47	721	Functions of FCC
47	901	**National Telecommunications and Information Administration Organization Act**
47	1001	**Communications Assistance for Law Enforcement Act of 1994** (See also amendments to 18 USC 2521 and sections of Title 47)
48	551	**Cable Communications Policy Act of 1984**
50	401	Privacy of National Security Information (See also Executive Order Number 12356)
50	401	Electronic surveillance, defined, U.S. intelligence activities (See also Executive Order Number 12333)
50	413	Congressional oversight of intelligence activities
50	1541	**War Powers Resolution Act**
50	1801 et seq.	**Foreign Intelligence Surveillance Act of 1978**
50	1801	Electronic surveillance, foreign intelligence purposes. Outside U.S.; actual or potential threat; ability of U.S. to protect against
50	1801	Electronic surveillance defined
50	1801	Consent
50	1802	Authorization of electronic surveillance without court order (See also Executive Order Number 12139)
50	1805	Approval of procedures for testing electronic surveillance equipment
50	1805	Authorization for electronic surveillance to determine existence and capability of equipment of non-authorized persons
50	1806	Disclosure of electronic surveillance methods to aggrieved party; harm to national security
50	1811	Authorization of electronic surveillance without court order; By President during time of War
50	2401 et seq.	**Export Administration Act of 1979**
50	2401 et seq.	Export of scientific and technical data
50	2510	Export of software or data controlled by DoD

Regulatory

Regulatory

REGULATORY DOCUMENTS
ANNOTATED BIBLIOGRAPHY

The following is an annotated bibliography of regulatory documents relevant to information warfare. Key words are also provided.

Code of Federal Regulations, Title 41, Chapter 201, *Federal Information Resources Management Regulation.*

KEY WORDS: Federal, IRM, Warner exempt

ABSTRACT: This chapter regulates the creation, maintenance, and use of Federal records and the acquisition, management and use of information processing systems. Warner exempt systems, radar, sonar, radio, and television systems are exempted.

Code of Federal Regulations, Title 47, Chapter 1, Part 63*, Rules to Provide for Notification by Common Carriers of Service Disruptions.*

KEY WORDS: FCC, NS/EP, outage reporting

ABSTRACT: This section of the Federal Communications Commission Rules and Regulations establishes outage reporting requirements and procedures. Common carriers are required to report outages potentially affecting 30,000 or more customers for 30 or more minutes. Also outages which affect special facilities, defined as 911 tandem switches, major airports, and NS/EP facilities are reported to the NCS.

Code of Federal Regulations, Title 47, Chapter II, Part 201-216, *Office of Science and Technology Policy and National Security Council.*

KEY WORDS: NS/EP, NCS, restoration priority, precedence

ABSTRACT: This chapter prescribes the conservation, allocation, and use of the Nation's telecommunications resources during crises and emergencies. It assigns responsibilities and includes NCS Directives.

Executive Office of the President, Executive Order 12333, *United States Intelligence Activities*, The White House, Washington DC, December 4, 1981.

KEY WORDS: SecDef, NSA, DoE, Attorney General, intelligence, counterintelligence, communications security

ABSTRACT: Intelligence effort to provide necessary information on which to base decisions to the President and to protect national interests from foreign security threats. Special emphasis to countering espionage directed against U.S. government, corporations, establishments or persons. Secretary of Defense named executive agent for signals intelligence and communications security activities. NSA to execute the responsibilities of the SecDef as executive agent for communications security. NSA to conduct research and development as necessary for signals intelligence and communications security. Department of Energy will support NSA as requested. Restricts collection techniques to procedures established by the agency head and approved by the Attorney General (See Foreign Intelligence Surveillance Act of 1978).

Executive Office of the President, Executive Order 12334, *President's Intelligence Oversight Board*, The White House, Washington DC, December 4, 1981.

KEY WORDS: Intelligence, oversight, national security, illegal

ABSTRACT: This order establishes the Intelligence Oversight Board and charges it with reviewing practices and procedures, investigating, and reporting to the President and the Attorney General any intelligence activities that any of the members believe to be in violation of the Constitution, laws, or presidential orders or directives. Heads of agencies, inspectors general, and general counsels will report intelligence activities they believe to be unlawful. Board members will be distinguished and trustworthy citizens outside of the government.

Executive Office of the President, Executive Order 12356, *National Security Information,* The White House, Washington DC, April 1, 1982 (Revoked).

KEY WORDS: National security information, classification, declassification

ABSTRACT: This EO prescribes a uniform policy for securing, classification and declassification of national security information. EO 12958 (see below) was issued on April 17, 1995 revoking this EO.

Executive Office of the President, Executive Order 12382, *President's National Security Telecommunications Advisory Committee*, The White House, Washington DC, September 13, 1982.

KEY WORDS: NSTAC, NCS

ABSTRACT: Established the NSTAC to provide the President advice and information from the perspective of industry with respect to national security telecommunications. OMNCS provides secretariat support.

Executive Office of the President, Executive Order 12472, *Assignment of National Security and Emergency Preparedness Telecommunications Functions,* The White House, Washington D.C., April 3, 1984.

KEY WORDS: NCS, NSTAC, COP, NS/EP

ABSTRACT: Established the National Communications System, an interagency group made up of 23 Federal departments and agencies. The NCS is responsible for ensuring that NS/EP telecommunications are available across a spectrum of national emergencies. NCS was to serve as a forum for government agencies and private sector. To facilitate this process, EO 12472 established the Committee of Principals for the Federal government to coordinate with the National Security Telecommunications Advisory Committee consisting of industry representatives.

Executive Office of the President, Executive Order 12881, The White House, Washington D.C.

KEY WORDS: NSTC, national goals, R&D

ABSTRACT: This EO established the National Science and Technology Council (NSTC) to establish goals for Federal science and technology investments in a number of areas including information technology. The NSTC is a cabinet -level body chaired by the President. It prepares R&D investment strategies targeting national goals that are coordinated across all Federal agencies.

Executive Office of the President, Executive Order 12958, *Classified National Security Information*, The White House, Washington D.C., April 17, 1995.

KEY WORDS: National security information, classification, declassification, OMB, GSA, ISOO

ABSTRACT: This EO revoked EO 12356. It has two major purposes: 1) To prevent unauthorized disclosure of information and 2) to prevent over-classification of information. It prescribes a uniform system for classifying, safeguarding, and declassifying national security information. The EO tasks OMB with issuing implementing directives in coordination with the USSPB and the Assistant to the President for National Security Affairs. It establishes within the OMB the Information Security Oversight Office (Previously an office in GSA) to implement and monitor the program on behalf of the Director, OMB. It also establishes the Information Security Policy Advisory Council. As a Federal Advisory Committee the Council is to advise the President and other members of the Executive Branch on security policies and provide recommendations to agency heads for specific subject areas for declassification review.

Federal Communications Commission, Notification of Service Outage, 47 C.F.R. 63.100.

KEY WORDS: PSN, outage, reporting

ABSTRACT: The purpose of this FCC Report and Order was to update a systematic means by which to monitor, on a timely basis, major telephone service outages throughout the nation. It required local and interexchange common carriers operating transmission or switching facilities and that provide access service or interstate or international service, to promptly notify the FCC of any outage of 30 minutes or more with the potential to affect 30,000 or more customers or that affect critical facilities such as major airports and important government facilities. This rule was published in the Federal Register on August 1994; it updates a 1992 rule.

Policy

Policy

POLICY DOCUMENTS
ANNOTATED BIBLIOGRAPHY

The following is an annotated bibliography of policy documents having applicability to information warfare/information assurance. Included are: National Security Decision Directives, National Security Directives, Presidential Decision Directives, Presidential Directives, NIST and NTIA standards and instructions, and the regulations, directives, and instructions of other organizations such as the Department of Defense. Key words are also provided. An "Index of Key Policy Documents" and an "Index of Key Implementation Standards, Guidelines, and Procedures" follow the annotated bibliographies.

Department of the Army, U.S. Army Training and Doctrine Command, *Concept for Information Operations--Final Coordinating Draft*, Jan 31, 95.

KEY WORDS: DoD, Army

ABSTRACT: Describes concept for information operations (IO), the environment, defines IO terms and relates IO to Force XXI operations.

Department of the Army, U.S. Army Training and Doctrine Command, FM 100-6, *Information Operations*, 15 April 1996.

KEY WORDS: DoD, Army

ABSTRACT: Capstone doctrinal document for incorporating information operations into "Army doctrine, individual and unit training, leader development, force design, and material acquisition initiatives."

Department of the Navy, OPNAV Instruction 3430.26, Chief of Naval Operations/N6, IW/C2W Implementing Instruction

KEY WORDS: DoD, Navy, IW/C2W, policy, joint, coordination, responsibilities, implementation

ABSTRACT: This instruction implements policy for the employment of Navy resources in support of IW/C2W and conforms to the guidance contained in previously issued directives (DoD Instruction TS3600.1, CJCS MOP 30, and OPNAVINST 3430.25). It updates previously-used terms, concepts and disciplines, and discusses the purposes of IW and C2W. The effectiveness of

IW/C2W employment is stressed. Responsibilities are delineated for: CNO (N1/2/3/4/5/6/7/ 8/09N/091/095); Chief of Naval Education and Training; Naval Systems Commands; Naval Doctrine Command; Naval Security Group Command; Fleet Information Warfare Center; Naval Information Warfare Activity; Naval Criminal Investigative Service; and Fleet CINCs.

Executive Office of the President, Presidential Directive/National Security Council 24, *Telecommunications Protection Policy (U)*, November 16, 1977 (Partially declassified/released on February 18, 1994), Washington D.C., U.S. Government Printing Office.

KEY WORDS: NSA, DoC, NCSC, sensitive information,

ABSTRACT: Created an NSC Special Coordinating Committee which was subsequently replaced by the NTISSC and then the NSTISSC. Gave DoD authority to safeguard sensitive information that "would be useful to an adversary." Made NSA responsible for all classified information and the Department of Commerce responsible for sensitive information.

National Institutes of Standards and Technology (NIST), NIST Special Publication 800-12, *An Introduction to Computer Security: The NIST Handbook,* U.S. Government Printing Office, October 1995.

KEYWORDS: NIST, management controls, operational controls, technical controls, computer security, data integrity, system integrity, availability, confidentiality, life cycle assurance, incident handling

ABSTRACT: This handbook provides a broad overview of computer security to help readers understand their computer security needs and develop a sound approach to the selection of appropriate security controls. It assists in securing computer-based resources (including hardware, software, and information) by explaining important concepts, cost considerations, and interrelationships of security controls. The handbook illustrates the benefits of security controls, the major techniques or approaches for each control, and important related considerations.

National Institutes of Standards and Technology (NIST), NIST Publications List 91, *Computer Security Publications,* October 1995. Electronically updated February 1996.

KEY WORDS: Index, COMPUSEC, NIST, publications

ABSTRACT: Index of computer security publications published by NIST/Computer Systems Laboratory. Includes special publications, reports, and

Federal Information Processing Standards (FIPS) with price list and ordering information.

National Institute of Standards and Technology (NIST), NIST Federal Information Processing Standards (FIPS) Publication 186, *Digital Signature Standard (DSS),* May 1994.

KEY WORDS: DSS, DSA, digital signature

ABSTRACT: This FIPS describes a digital signature algorithm for use in applications that require both a guarantee of the identity of an originator and of the data integrity.

National Institute of Standards and Technology (NIST), NIST Federal Information Processing Standards (FIPS) Publication 190, *Guideline for the Use of Advanced Authentication Technology Alternatives*, September 28, 1994.

KEY WORDS: authentication, passwords, tokens, biometrics, COMPUSEC

ABSTRACT: This FIPS addresses alternatives to the standard use of passwords to prevent unauthorized access to computer systems. It covers authentication tokens and biometric devices.

National Institute of Standards and Technology (NIST), NIST Federal Information Processing Standards (FIPS) Publication 191, *Guideline for the Analysis of Local Area Network Security*, November 9, 1994.

KEY WORDS: COMPUSEC, LAN

ABSTRACT: This FIPS describes a security architecture for Local Area Networks, threats and vulnerabilities and security techniques.

National Institute of Standards and Technology, (NIST), NIST Internal Report Number 5424, *A Study of Federal Agency Needs for Information Technology Security*, May 1994.

KEY WORDS: DoC, DoEd, DoJ, NASA, SSA, requirements, Federal, INFOSEC

ABSTRACT: This NIST report documents the results of a study of the INFOSEC needs of the Department of Commerce, Department of Education, Department of Justice, NASA, and the Social Security Administration.

National Institute of Standards and Technology, (NIST), NIST Special Publication 800-9, *Good Security Practices for Electronic Commerce, Including Electronic Data Interchange*, December 1993.

KEY WORDS: NIST, EC/EDI

ABSTRACT: This NIST special publication was sponsored by the Farmers Home Administration. It addresses good security practices that should be considered when developing an EC/EDI system.

National Institutes of Standards and Technology (NIST), NIST Special Publication 800-11, *The Impact of the FCC's Open Network Architecture on NS/EP Telecommunications Security,* U.S. Government Printing Office, February 1995.

KEY WORDS: NIST, FCC, telecommunications security, National Security/Emergency Preparedness

ABSTRACT: This report provides an overview of the Federal Communications Commission's Open Network Architecture (ONA), describes National Security and Emergency Preparedness (NS/EP) telecommunications security concerns and details NS/EP telecommunications security concerns that the FCC's ONA requirement introduces into the Public Switched Network (PSN).

National Institute of Standards and Technology (NIST), NIST Special Publication 800-10, *Keeping Your Site Comfortably Secure: An Introduction to Internet Firewalls,* U.S. Government Printing Office, Washington, 1994.

KEY WORDS: NIST, firewalls, Internet

ABSTRACT: This NIST special publication provides an overview of the Internet, Internet security problems and firewalls. It is written in an elementary, non-technical style and refers the reader to sources of additional information.

National Institutes of Standards and Technology (NIST),NIST Special Publication 800-13, *Telecommunications Security Guidelines for Telecommunications Management Network,* U.S. Government Printing Office, October 1995.

KEYWORDS: NIST, telecommunications management network, telecommunications security, security threats, network elements and mediation devices

ABSTRACT: This guideline is intended to provide a security baseline for network elements (NEs) and mediation devices (MDs) that is based on commercial security needs. Some National Security/Emergency Preparedness (NS/EP) security required will be integrated into the baseline to address specific

network security needs. This publication is the first of a series of Telecommunications Security Guidelines (TSG) that may be produced to address a hierarchy of telecommunications architectures of increasing complexity.

National Institutes of Standards and Technology (NIST), *Generally Accepted Principles and Practices for Security Information Technology Systems (Draft),* December 18, 1995. (Final Due to be Published in late July 1996)

KEY WORDS: NIST, Information Technology, Information Technology Security, Information Technology Security Principles, Information Technology Security Practices

ABSTRACT: This draft document provides a baseline that can be used to establish and review Information Technology (IT) security programs. Management, internal auditors, users, system developers, and security practitioners can use the guideline to gain an understanding of the basic security requirements applicable to most IT systems. The security principles and practices are to be applied in the use, protection, and design of government information systems, particularly front-line systems for delivering services in an electronic form.

National Security Agency (NSA), National Telecommunications and Information Systems Security Directive No. 600, *Communications Security Monitoring*, April 10, 1990.

KEY WORDS: COMSEC monitoring, government telecommunications, privacy

ABSTRACT: States that government telecommunications systems are subject to monitoring by authorized government agencies. Applies to official telecommunications of Federal government employees, contractors, and other entities when transmitted over government owned or leased telecommunications systems. Government telecommunications and telecommunications systems defined.

National Security Decision Directive (NSDD) 145, 1984.

KEY WORDS: NSTISSC, EOP, unclassified information

ABSTRACT: Created (reestablished) the interagency group National Security Telecommunications and Information Systems Security Committee (NSTISSC) and required protection of sensitive unclassified information as well as classified information. NSDD 145 was rescinded by NSD 42.

National Security Decision Directive (NSDD) 298, 1988.

KEY WORDS: Policy, EOP, directive, OPSEC, NSA, IOSS

ABSTRACT: Mandated implementation of a formal OPSEC program by each executive department and agency with national security responsibilities. Designated Director, NSA, as executive agent for OPSEC programs and tasked him to establish and maintain an Interagency OPSEC Support Staff (IOSS).

National Security Directive 42, July 5, 1990.

KEY WORDS: SecDef, NSA, NSTISSC, COP, CIA, COMSEC monitoring, National Manager, vulnerability, Federal government

UNCLASSIFIED ABSTRACT: NSD 42 revised NSDD 145 with the objective of improving U.S. government capabilities for securing national security systems against technical exploitation and implementing countermeasures. SecDef is executive agent and Director, NSA designated as the National Manager and charged with examining national security systems and evaluating their vulnerability. Defines telecommunications, information systems, and national security systems. Reestablishes the national Security Telecommunications and Information Systems Security Committee (NSTISSC). NSTISSC is tasked to develop policies, procedures, guidelines, instructions, standards, objectives, and priorities and systems security guidance, approve the release of cryptographic material to foreign governments with CIA concurrence, establish a national system for promulgating operating policies, instructions, directives, guidance, etc. and to interact with the National Communications Systems Committee of Principals established by Executive Order 12472. NSA provides a supporting secretariat.

Office of Management and Budget (OMB), Circular A-123 (Revised), *Management Accountability and Control*, Executive Office of the President, Publication Services, June 21, 1995.

KEYWORDS: OMB, management accountability, management control

ABSTRACT: This Circular replaces Circular No. A-123 "Internal Control Systems" revised, dated August 4, 1986 and OMB's 1982 "Internal Control Guidelines". This revised Circular provides guidance to Federal managers on improving accountability and effectiveness of Federal programs and operations by establishing, assessing, correcting, and reporting on management controls. This Circular provides policy for management accountability and management controls and the attendant actions required.

Office of Management and Budget (OMB), Circular A-130 (Revised by Transmittal Memorandum No. 3), *Management of Information Resources,* Washington, D.C., February 8, 1996.

KEYWORDS: OMB, Federal Government, policy, security, security plans

ABSTRACT: This Circular establishes policy for the Management of Federal Information Resources. Specific procedural and analytic guidance is provided in Appendix III (*Security of Federal Automated Information Resources)* for implementing Federal automated information security programs, assignment of agency responsibilities for security of automated information, and links agency automated information security programs and agency management control systems established in accordance with OMB Circular A-123.

Appendix III revised procedures contained in the original A-130 Appendix III and incorporates requirements contained in the Computer Security Act of 1987 (P.L. 100-235) and responsibilities assigned in applicable national security directives. Agency programs shall include the following controls in general support systems and major applications.

General Support Systems: Assign Responsibility for Security; Develop and Implement a System Security Plan as part of the organization's IRM planning process; Review the Security Controls (at least every three years or when significant modifications are made to the system); and, Ensure that a Management Official Authorizes in Writing the Use of Each System (before beginning or significantly changing processing in the system).

Major Applications: Assign Responsibility for Security; Develop and Implement a System Security Plan; Perform an Independent Review or Audit of the Security Controls (at least every three years); and, Ensure that a Management Official Authorizes in Writing the Use of the Application.

Office of Management and Budget (OMB*),* Circular A-130 (Revised)*, Policy on Open Systems.*

KEY WORDS: OMB, Federal government, policy, security

ABSTRACT: The revised A-130, a capstone federal information systems policy document, provides uniform government-wide information resources management policies. A-130 is being revised in phases. Transmittal Memorandums Number 1 (June 25, 1993) and 2 (July 25, 1994) have been issued. Appendix III, Security has been published for comment. The Appendix III revision aligns Federal government security responsibilities with the Computer Security Act. It requires assignment of security responsibilities, requires security plans for all general support computer systems and stresses management controls and risk management.

Office of Management and Budget (OMB), National Information Infrastructure Security Issues Forum, *NII Security: The Federal Role,* Washington DC, June 14, 1995.

KEY WORDS: OMB, NII, IITF, security, federal role

ABSTRACT: The Security Issues Forum and the U.S. Advisory Council (NII) held seven public meetings with government officials and representatives of the public and private sector. Users and service providers were represented at these meetings. The feedback received at these meetings has been incorporated into this report. The report, issued for comment, "summarizes the Forum's findings concerning security needs in the National Information Infrastructure (NII); presents an analysis of the institutional, legal, and technical issues surrounding security in the NII; and proposes Federal actions to address these issues." The report defines security in the NII to include integrity, availability, and confidentiality of information and reliability of systems. Findings for action include: (1) adoption of the proposed NII Security Tenets, (2) adoption for the NII of the Organization for Economic Cooperation and Development (OECD) Security Principles, and (3) implementation of the Federal role as recommended in the report. Federal roles include stimulating security issues dialogue and awareness, making Federal security products and techniques available for use on the NII, and promoting private sector development of security products and services. Additionally, "In its role as protector of the public interest, the government will: (1) assure adequate emergency response capability on the NII; (2) adapt current oversight processes to meet the challenges of the NII; (3) review criminal law; and (4) promote international cooperation.

Office of the Secretary of Defense, DoD Directive 8000.1, *Defense Information Management Program*, October 27, 1992.

KEY WORDS: DoD, policy

ABSTRACT: Director, DISA will "in consultation with the Directors of the DIA and NSA, provide technology and services to ensure the availability, reliability and maintainability, integrity, and security of defense information, commensurate with its intended use."

INDEX OF KEY POLICY DOCUMENTS

Policy Documents
Air Force Regulation 205-16 (superseded by AFSSI 5100)
Air Force Regulation 56-1 (superseded by AFSSI 4100)
Air Force Regulation 57-1, Operational Needs, Requirements, and Concepts
Air Force Regulation 400-26, Logistics Support for Ground Communications-Electronic Systems and Equipment
Air Force Regulation 700-1, Managing Air Force Communications-Computer Systems
Air Force Regulation 700-2, Communications-Computer Systems Planning and Architectures
Air Force Regulation 700-3, Information Systems Requirements Processing
Air Force Regulation 700-4, Volume I: Information Systems Program Management, Volume II: Information System Acquisition and Major Automated Information Systems Review Requirements
Air Force Regulation 800-1, Air Force Acquisition System
Air Force Instruction 31-40, Information Security Program Management
Army TRADOC, PAM 525-XX, Concept for Information Operations, Final Coordinating Draft
Army TRADOC, FM 100-6, Information Operations, Coordinating Draft
Army Regulation 380-19, Information Systems Security
Army Regulation 380-5
Army Regulation 380-40, Policy for Safeguarding and Controlling COMSEC Material
Army Regulation 525-20
Army Regulation 25-1, The Army Information Resources Management Program
Army Regulation 25-3, Army Life Cycle Management of Information Systems
Army Regulation 70-1, Army Acquisition Policy
CJCS, National Military Strategy Document, App. C, C4 Systems
CJCS MOP 3, Command, Control, & Communications Countermeasures
CJCS MOP 6, Electronic Warfare
CJCS MOP 10, Near Real Time Analysis of EMI and Jamming of U.S. Space Systems
CJCS MOP 24, Tactical Employment of Directed Energy Combat Systems
CJCS MOP 30, Command and Control Warfare
CJCS MOP 43, Military Telecommunications Agreements and Arrangements between the U.S. and Regional Defense Organizations or Friendly Foreign Nations
CJCS MOP 52, Policy and Responsibilities for the Denial of Environmental Information to an Enemy
CJCS MOP ??, Information Resource Management
CJCS Instruction 6211.02, Defense Information System Network and Connected Systems
CJCS Instruction 6212.01, Compatibility, Interoperability, and Integration of C3I Systems
CJCS Instruction 6510.1, Joint and Combined Communications Security
CJCS, Joint Pub 1, Joint Warfare of the U.S. Armed Forces
CJCS, Joint Pub 1-02, Dictionary of Military Terms
CJCS, Joint Pub 3-13, Doctrine for Command and Control Warfare (C2W)
CJCS, Joint Pub 3-53, Doctrine for Joint Psychological Operations

CJCS, Joint Pub 3-54, Joint Doctrine for Operations Security
CJCS, Joint Pub 3-58, Joint Doctrine for Military Deception
COMSEC Program Publications, Various DoD, NSA
Federal Information Resources Manual (IRM)
Marine Corps Order 3430.5A, Policy for Command & Control Warfare (C2W)
Marine Corps Publication 5510.14, Marine Corps Automatic Data Processing Security Manual
NCSC Policy 1, National Policy for Safeguarding and Control of Communications Security Material
NCSC Policy 2, National Policy on Release of Communications Security Information to U.S. Contractors and Other U.S. Nongovernment Sources
NCSC Policy 3, TEMPEST Glossary
NCSC Policy 5, National Policy on Use of Cryptomaterial by Activities Operating in High Risk Environments
NCSC Policy 6, National Policy Governing the Disclosure or Release of Communications Security Information to Foreign Governments and International Organizations
NCSC Policy 8, National Policy on Secure Voice Communications
NCSC Policy 11, Policy for National Security Information Carried by Any Transmission System By Government or Contractors
Naval Doctrine Publication 1, Naval Warfare, Volume 6, Command and Control
Navy, OPNAVINST 3430.25, Information Warfare and Command and Control Warfare
Navy, OPNAVINST 3430.26, Implementing Instruction fro Information Warfare (IW)/Command and Control Warfare (C2W)
Navy, OPNAVINST 5239.1A, Department of the Navy ADP Security Manual
Navy, OPNAVINST 5290.1A, Naval Imaging Program Policy and Responsibility
Navy, OPNAVINST 5510.1H, Department of the Navy Information and Personnel Security Program Regulation
Navy, OPNAVINST C5510.93E, Navy Implementation of National Policy on Control of Compromising Emanations
Navy, OPNAVINST 5530.14B, Department of the Navy Physical Security and Loss Prevention Manual
Navy, SECNAVINST 5000.2A, Implementation of Defense Acquisition Management Policy-Procedures Documentation and Report
Navy, SECNAVINST 5200.32A, Acquisition Management Policies and Procedures for Computer Resources
Navy, SECNAVINST 5231.1C, Life Cycle Management Policy and Approval Requirements for Information System Projects
Navy, SECNAVINST 5233.1B, Department of the Navy Automated Data Systems Documentation Standards
Navy, SECNAVINST 5238.1C, Computer Resources Management
Navy, SECNAVINST 5239.2, Department of the Navy AIS Security Program
Navy, SECNAVINST 5400.15, Department of the Navy Research, Development, and Acquisition Responsibilities
Navy, SECNAVINST 5510.30, Department of the Navy Personnel Security Program

NSA, National Policy for the Security of National Telecommunications and Information Systems
NSD 42, (Revised NSDD 145)
NSDD 97, National Security Telecommunications Policy
NSDD 145, Protection of Both Classified and Sensitive Information; Interagency Structure for Computer Security
NSDD 189, Reporting of Unclassified Research
NSDD 298
OMB Circular A-119, Federal Participation in the Development and Use of Voluntary Standards
OMB Circular A-123, Internal Control Systems
OMB Circular A-127, Financial Management Systems
OMB Circular A-130, Management of Federal Information Resources
OSD, Defense Management Review Decision (DMRD) 918
OSD, DoD Directive 3222.4, Electronic Warfare and Command and Control Warfare (C2W) Countermeasures
OSD, DoD Directive TS 3600.1, Information Warfare
OSD, DoD Directive 4640.6, Communication Security Telephone Monitoring and Recording
OSD, DoD Directive 5000.1, Defense Acquisition
OSD, DoD Directive 5100.1, Functions of the DoD and Its Major Components
OSD, DoD Directive 5100.30, World-wide Military Command and Control System (WWMCCS)
OSD, DoD Directive 5105.19, Defense Information Systems Agency
OSD, DoD Directive 5200.1, DoD Information Security Program
OSD, DoD Directive C-5200.2, Department of Defense Personnel Security Program
OSD, DoD Directive C-5200.5, Communications Security (COMSEC)
OSD, DoD Directive C-5200.8, Security of DoD Installations and Resources
OSD, DoD Directive S-5200.16, Objectives and Minimum Standards for Communications Security Measures used in Nuclear Command, Control, and Communications
OSD, DoD Directive C-5200.19, Control of Compromising Emanations
OSD, DoD Directive 5200.28, Security Requirements for Automated Information Systems
OSD, DoD 5200.28-STD, DoD Trusted Computer System Evaluation Criteria
OSD, DoD Directive 5205.2, DoD Operations Security Program
OSD, DoD Directive O-5205.7, Special Access Program Policy
OSD, DoD Directive C-5215.1
OSD, DoD Directive 5220.22, DoD Industrial Security Program
OSD, DoD Directive 5240.11, Damage Assessments
OSD, DoD Directive 7750.5, Management and Control of Information Requirements
OSD, DoD Directive 8000.1, Defense Information Management Program
OSD, DoD Directive 8320.1, DoD Data Administration
OSD, DoD Regulation 5200.1-R, Information Security Program Regulation
OSD, DoD Manual 5000.2-M, Defense Acquisition Management Documentation and Reports
OSD, DoD Manual 5200.28-M, Automated Information System Security Manual

OSD, DoD Manual 8020.1-M Management Guidance on Functional Process Improvement
OSD, DoD Instruction 5000.2, Defense Acquisition Management Policies and Procedures
OSD, DoD Instruction 5240.11, Damage Assessments
OSD, DoD Instructions, 8000 Series Information Management
8000-8099 Defense Information Management
8100-8199 Information Systems
8200-8299 Information Services
8300-8399 Data Management
8400-8499 Information Technology
8900-8999 Information Collection and Dissemination
OSD, DoD Instruction 8000.2, Defense Information Management Policies and Procedures
OSD, DoD Instruction 8020.1, Functional Process Improvement Program
Presidential Directive/National Security Council 24
Presidential Directive 53, National Security Telecommunications Policy

INDEX OF KEY IMPLEMENTATION STANDARDS, GUIDELINES, AND PROCEDURES

Implementation Standards, Guidelines, and Procedures
COMSEC Program Publications
Summary of the Commercial COMSEC Endorsement Program (CCEP)
Handling and Control of Controlled Cryptographic Items During Development and Manufacture/Assembly
Industrial Security Manual for Safeguarding Classified Information (DoD 5220.22-M)
COMSEC Supplement to DoD Industrial Security Manual (DoD 5220.22-S)
Industrial COMSEC Material Control Manual
U.S. Government Contractors Controlled Cryptographic Item (CCI) Manual
DCID 1/16 Handling of Intelligence Information
DIA, Security Requirements for System High and Compartmented Mode Workstations
DIA, Compartmented Mode Workstation Evaluation Criteria
DIA, Compartmented Mode Workstation Standard user Interface Style Guide
DIA Manual 50-3
DIA Manual 50-4
DIA Manual 50-5
DIA Manual 50-6
DIA Manual 50-8
DIA Manual 50-24
DIA Manual 50-28
National Communications Security (COMSEC) Instructions (NACSI), 12 Titles
National Communications Security (COMSEC) Information Memoranda (NACSIM), 3 Titles
National Communications Security (COMSEC) Emanations Memoranda (NACSEM), 9 Titles
NIST, FIPSPUB 31 Guidelines for ADP Physical Security and Risk Management
NIST, FIPSPUB 39, Glossary for Computer Systems Security
NIST, FIPSPUB 41, Computer Security Guidelines for Implementing the Privacy Act of 1974
NIST, FIPSPUB 46-1, Data Encryption Standard
NIST, FIPSPUB 48, Guidelines on Evaluation of Techniques for Automated Personal Identification
NIST, FIPSPUB 65, Guideline for Automated Data Processing Risk Analysis
NIST, FIPSPUB 73, Guidelines for Security of Computer Applications
NIST, FIPSPUB 74, Guidelines for Implementing and using the NBS Data Encryption Standard
NIST, FIPSPUB 81, DES Modes of Operations
NIST, FIPSPUB 83, Guideline on User Authentication Techniques for Computer Network Access Control
NIST, FIPSPUB 87, Guidelines for ADP Contingency Planning
NIST, FIPSPUB 88, Guideline on Integrity Assurance and Control in Database Administration

NIST, FIPSPUB 94, Guideline on Electrical Power for ADP Installations
NIST, FIPSPUB 102, Guidelines for Computer Security Certification and Accreditation
NIST, FIPSPUB 112, Standard on Password Usage
NIST, FIPSPUB 113, Standard on Computer Data Authentication
NIST, FIPSPUB 139, Interoperability and Security Requirements for Use of the Data Encryption Standard in the Physical Layer of Data Communications
NIST, FIPSPUB 140, General Security Requirements for Equipment Using the Data Encryption Standard
NIST, FIPSPUB 141, Interoperability and Security Requirements for Use of the Data Encryption Standard with CCITT Group 3 Facsimile Equipment
NIST, FIPSPUB 179, Government Network Management Profile
NIST, FIPSPUB 185, Escrowed Encryption Standard
NIST, FIPSPUB 186, Digital Signature Standard
NIST, FIPSPUB 188, Standard Security Label for Information Transfer
NIST FIPSPUB 190, Guideline for the Use of Advanced Authentication Technology Alternatives
NIST FIPSPUB 191, Guideline for the Analysis of Local Area Network Security
NIST Internal Report 5424, A Study of Federal Agency Needs for Information Technology Security
NIST Special Publications, Various Titles
NSA, National Computer Security Center, Rainbow Series, Various Titles
NTISS/NSTISS Directive 500, Information Systems Security (INFOSEC) Education, Training, and Awareness
NTISS/NSTISS Directive 501, National Training Program for Information Systems Security (INFOSEC) Professionals
NTISS/NSTISS Directive 502, National Security Telecommunications and Automated Information Systems Security
NTISS/NSTISS Directive 503, Incident Response and Vulnerability Reporting for National Security Systems
NTISS/NSTISS Directive 600, Communications Security Monitoring
NTISS/NSTISS Directive 900, Governing Procedures of the National Security Telecommunications and Information System Security Committee (NSTISSC)
NTISS/NSTISS Directive 901, National Telecommunications and Information Systems Security Issuance System
NTISS/NSTISS Instructions 3000-3020 (21 Titles), Operational Security Doctrine for Various Cryptographic-Based Systems
NTISS/NSTISS Instruction 4000, Communications Security Equipment Maintenance and Maintenance Training
NTISS/NSTISS Instruction 4001, Controlled Cryptographic Items (CCI)
NTISS/NSTISS Instruction 4002, Classification Guide for COMSEC Information
NTISS/NSTISS Instruction 4003, Reporting and Evaluating COMSEC Incidents

NTISS/NSTISS Instruction 4004, Routine Destruction and Emergency Protection of COMSEC Material
NTISS/NSTISS Instruction 4005, Control of Top Secret Keying Material
NTISS/NSTISS Instruction 4006, Controlling Authorities for COMSEC Material
NTISS/NSTISS Instruction 4007, COMSEC Utility Program
NTISS/NSTISS Instruction 4008, Program for the Management and Use of National Reserve Information Systems Security (INFOSEC) Material
NTISS/NSTISS Instruction 4009, National Information Systems Security (INFOSEC) Glossary
NTISS/NSTISS Instruction 4010, Keying Material Management
NTISS/NSTISS Instruction 4011, National Training Standard for INFOSEC Professionals
NTISS/NSTISS Instruction 7000, TEMPEST Countermeasures for Facilities
NTISS/NSTISS Instruction 7001, NONSTOP Countermeasures
NTISS/NSTISS Policy 1, National Policy on Application of Communications Security to U.S. Civil and Commercial Space Systems
NTISS/NSTISS Policy 3, National Policy for Granting Access to U.S. Classified Cryptographic Information
NTISS/NSTISS Policy 4, National Policy on Electronic Keying
NTISS/NSTISS Policy 5, National Policy for Incident Response and Vulnerability Reporting for National Security Systems
NTISS/NSTISS Policy 8, National Policy on Certification and Accreditation of National Security Telecommunications and Information Systems
NTISS/NSTISS Policy 100, National Policy on Application of Communications Security to Command Destruct Systems
NTISS/NSTISS Policy 200, Controlled Access Protection (C2 by '92)
NTISS/NSTISS Policy 300, National Policy on Control of Compromising Emanations
NTISS/NSTISS Advisory Memoranda (NSTISSAM), 3 Titles, COMSEC Advisories
NTISS/NSTISS Advisory Memoranda (NSTISSAM), 4 Titles, COMPUSEC Advisories
NTISS/NSTISS Advisory Memoranda (NSTISSAM), 6 Titles, TEMPEST Advisories
OMB Bulletin 90-08, Guidance for Preparation of Security Plans for Federal Computer Systems that Contain Sensitive Information
OMB Bulletin 91-10, Information Resources Management (IRM) Plans Bulletin
OMB Bulletin 92-05, Information Resources Management (IRM) Plans Bulletin
OMB, OMB Bulletin 88-16, Guidance for Preparation and Submission of Security Plans for Federal Computer Systems Containing Sensitive Information
Other Security-Relevant Government Publications
OTA, Defending Secrets, Sharing Data: New Locks and Keys for Electronic Information
OTA, Federal Government Information Technology: Management, Security, and Congressional Oversight
OTA, Federal Government Information Technology: Electronic Surveillance and Civil Liberties
OTA, Federal Government Information Technology: Electronic Record Systems and Individual Privacy

TEMPEST Program Publications
NSA Objective Standards for Product Assurance
Endorsed TEMPEST Products Program
Endorsed TEMPEST Test Services Program
Endorsed TEMPEST Test Instrumentation Program
PPL Product Transition Guidelines and Procedures
PPL Accreditation Standard Operating Procedures and Requirements
ITP Quality Assurance Procedures
ITP Standard Operating Procedures

Additional Resources

Additional Resources

ADDITIONAL RESOURCES

Note: This list was compiled to provide the reader with additional resources for the topics covered in this document. Where appropriate, on-line resources have also been provided. For a more comprehensive compilation of information warfare resources, see National Defense University, School of Information Warfare and Strategy, *"Information-Based Warfare: An Annotated Bibliography."*

Introduction:

Arquilla, John & Ronfeldt, David., *"Cyberwar and Netwar: Warfare Between the Networks."*, Comparative Strategy. vol 12, no. 2, 1993, 141-165.

Campen, Alan D., *The First Information War: The Story of Communications, Computers, and Intelligence Systems in the Persian Gulf War.*

Government Accounting Office, *Information Security: Computer Attacks at Department of Defense Pose Increasing Risk*, GAO/AIMD-96-84, May, 1996

Libicki, Martin C., *What is Information Warfare?,* National Defense University Press, Washington, DC, 1995

National Defense University, School of Information Warfare and Strategy, *Information-Based Warfare: An Annotated Bibliography.*

Schwartau, Winn, *Information Warfare, Chaos on the Electronic Superhighway,* Thunder's Mouth Press, New York, 1994.

Sullivan, General Gordon R. & Dubik, Colonel James M., *"War in the Information Age."* Strategic Studies Institute, U.S. Army War College, June 6, 1994.

Toffler, Alvin and Heidi, *War and Anti-War; Survival at the Dawn of the Twenty-first Century*, Little, Brown and Company, Boston.

Infrastructures:

Agudo, Dr. Michael E., P.E., *An Overview of Electrical Power System Operation, Joint Program Office Special Technical Countermeasures*, March, 1996.

Bell Communications Research, *Generic Requirements for Data Communication Network Security,* Bellcore, New Jersey, January 1, 1994.

Computer Science and Telecommunications Board, National Research Council, *The Changing Nature of Telecommunications/Information Infrastructure,* National Academy Press, Washington DC, 1995.

Defense Information Systems Agency, *Defense Information Infrastructure Master Plan, Version 2.0,* Arlington, VA, March 20, 1995.

Office of the Manager, National Communications System, *The Electronic Intrusion Threat to National Security and Emergency Preparedness Telecommunications, An Awareness Document,* Arlington, VA, December 5, 1994.

On-line:

NII Researchers Site: http://www.pitt.edu/~malhotra/NII.htm
Information Infrastructure links: http://www.ansi.org/iisp/links.html

Legal, Regulatory, and Policy:

Communications Law--Compilation of Selected Acts Within the Jurisdiction of the Committee on Commerce, U.S. Government Printing Office, Washington DC, 1995.

Froomkin, Michael A., "The Metaphor is the Key: Cryptography, the Clipper Chip, and the Constitution."

Icove, David, Seger, Karl, & VonStorch, William, *Computer Crime: A Crimefighter's Handbook*, O'Reilly, 1995.

Interagency Working Group on Cryptography Policy, *Enabling Privacy, Commerce, Security and Public Safety in the Global Information Infrastructure* (Draft), May 20, 1996.

National Research Council, *Cryptographies Role in Security the Information Society,* Prepublication copy, May 30, 1996.

National Research Council, *The Changing Nature of Telecommunications/ Information Infrastructure*, National Academy Press, Washington, DC, 1995.

Office of Management and Budget, *Circular No. A-130: Management of Federal Information Resources*, Revised, February 8, 1996.

Office of Technology Assessment, *Information Security and Privacy in Network Environments,* OTA-TCT-606, U.S. Government Printing Office, Washington DC, 1994.

Office of Technology Assessment, *Issue Update on Information Security and Privacy in Network Environments,* OTA-BP-ITC-147, U.S. Government Printing Office, Washington, DC, 1995.

On-line:

Thomas legislative server: http://thomas.loc.gov
House law server: http://law.house.gov
Cornell U.S. Code archive: http://www.law.cornell.edu/uscode/
Telecomm Act of 1996 summary: http://www.clark.net/techlaw/act_summary.html
NRC Cryptography Report: http://www2.nas.edu/cstbweb/2646.html
Code of Federal Regulations:
http://thorplus.lib.purdue.edu/vlibrary/reference/gpo/index.html

Technology:

Cheswick, William and Steven Bellovin, *Firewalls and Internet Security; Repelling the Wily Hacker,* Addison-Wesley, Massachusetts, 1994.

DeLanda, Manuel, *War in the Age of Intelligent Machines*, The MIT Press, New York, 1991.

Munro, Neil, *The Quick and the Dead--Electronic Combat and Modern Warfare,* St, Martins Press, New York, 1991.

van Crevald, Martin, *Technology and War: From 2000 B.C. to the Present*, Free Press, New York, 1991.

Intelligence Issues:

U.S. Congress, Commission on the Roles and Capabilities of the United States Intelligence Community, *Preparing for the 21st Century: An Appraisal of U.S. Intelligence*, March 1, 1996.

General Accounting Office, *Computer Security: Hackers Penetrate DoD Computer Systems,* GAO/IMTEC-92-5, U.S. Government Printing Office, Washington DC, November, 1991.

Littman, Jonathan, *The Fugitive Game: On-line with Kevin Mitnick*, Little, Brown and Company, New York, 1996.

Quittner, Joshua & Slatta, Michelle, *Masters of Deception: the Gang that Ruled Cyberspace*, New York, HarperCollins, 1995.

Sterling, Bruce, *The Hacker Crackdown: Law and Disorder on the Electronic Frontier*, New York, Bantam Books, 1992.

Stoll, Clifford, *The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage,* Random House, New York, 1992.

On-line:

Internet Underground: http://underground.org/

Doctrine:

Department of Defense, TS 3600.1, *Information Warfare (U)*, December 21, 1992.

Department of the Air Force, "Cornerstones of Information Warfare," Whitepaper, 1995.

Department of the Navy, "COPERNICUS...FORWARD, C4I for the 21st Century."

Department of the Navy, OPNAVINST 3430.26: *Implementing Instruction for IW/C2W*, January 18, 1995.

Headquarters, Department of the Army, *C2 Protect Program Management Plan*, vol. 1, August 1995.

Headquarters, Department of the Army, Training and Doctrine Command, *FM 100-6: Information Operations*, April 15, 1996

References

References

REFERENCES

[BELLCORE] BELLCORE, Inc., *Security in Broadband Networks Briefing*, John F. Kimmins, Information Infrastructure Standards Panel Meeting, March 27-28, 1996.

[CHINA] *Jiefangjun Bao'*, Beijing, in Chinese, April 16, 1996.

[CIWG] Report of the Critical Infrastructure Working Group*: Options for Protecting Critical National Infrastructures*, February 6, 1996.

[CJCS] Chairman, Joint Chiefs of Staff, *CJCSI 6510.01 (Draft),* March 8, 1996.

[DARPA] Defense Advanced Research Projects Agency, *Information Science and Technology (ISAT) 1995 Summer Study on Survivable Distributed Information Systems Briefing (DARPA Internal Study)*, 1995.

[DISA 1] Defense Information Systems Agency, *Protecting the Defense Information Infrastructure; DISA Defensive Information Warfare Management Plan (Draft Version 4.1),* May 23, 1996.

[DISA 2] Defense Information Systems Agency, DoD Regulatory Council - Telecommunications, *Telecommunications Act of 1996: Summary Fact Sheet*, 1996.

[FCW] *Federal Computer Week, Special Report: Bosnia, The Role of I.T. in Operation Joint Endeavor*, Supplement to Federal Computer Week, April 29, 1996.

[FEMA] Federal Emergency Management Agency, *Federal Emergency Response Plan,*

[GAO] Government Accounting Office, *Information Security: Computer Attacks at Department of Defense Pose Increasing Risk,* GAO/AIMD-96-84, May, 1996

[HQDA 1] Headquarters, Department of the Army, C2 Protect Program Management Plan, vol. 1, August 1995

[HQDA 2] Headquarters, Department of the Army, Training and Doctrine Command, *FM 100-6: Information Operations*, April 15, 1996

[IDA 1] Institute for Defense Analyses, *Information Warfare Technologies: Survey of Selected Civil Sector Activities*, IDA Document D-1792, February, 1996

[IDA 2] Institute for Defense Analyses, *Information Warfare: Selected Long-Range Technology Applications*, IDA Paper p-3157, February, 1996.

[IITF] Information Infrastructure Task Force, *The National Information Infrastructure: Agenda for Action,* September 15, 1993

[JP0 1] Joint Program Office for Special Technical Countermeasures, *An Overview of Electrical Power System Operation*, Agudo, Dr. Michael E., P.E, March, 1996.

[JPO 2] Joint Program Office for Special Technical Countermeasures, *Infrastructure Assurance*, Briefing by Ms. Susan Hudson and Mr. Robert Podlesney to the Defense Science Board, March 12, 1996.

[JS] Joint Staff, Information Warfare Division (J6K), *Mission Need Statement for Infrastructure Assurance Modeling (Draft)*, February 29, 1996.

[KEMA-ECC] KEMA-ECC, Inc., *Electric Utility Controls and Exposure to Security Threats,* Briefing by Mr. Joseph Bucciero to the NSTAC IATF Energy Risk Assessment Subgroup, June 6, 1996.

[NIST] National Institute of Standards and Technology, *The Impact of the FCC's Open Network Architecture on NS/NP Telecommunications Security*, NIST Special Publication 800-11, February 1995.

[NRC] National Research Council, *Growing Vulnerability of the Public Switched Networks*, National Academy Press, 1989.

[NSTAC 1] National Security Telecommunications Advisory Committee, *An Assessment of the Risk to the Security of the Public Network*, Network Security Information Exchange, December, 1995.

[NSTAC 2] National Security Telecommunications Advisory Committee, *Information Assurance Task Force Plan*, Briefing to the NSTAC, February 28, 1996.

[OMB] Office of Management and Budget, *NII Security: The Federal Role*, June 5, 1995

[OTA 1] Office of Technology Assessment, *Information Security and Privacy in Network Environments,* OTA-TCT-606, U.S. Government Printing Office, Washington DC, 1994.

[OTA 2] Office of Technology *Assessment, Issue Update on Information Security and Privacy in Network Environments*, OTA-BP-ITC-147, U.S. Government Printing Office, Washington, DC, 1995.

[RVWG] Reliability and Vulnerability Working Group, Telecommunications Policy Committee, Information Infrastructure Task Force, *NII Risk Assessment: A Nation's Information at Risk*, February 29, 1996.

[USAC] United States Advisory Council on the National Information Infrastructure, *A Nation of Opportunity: Realizing the Promise of the Information Superhighway*, January, 1996.

[USAF] Department of the Air Force, "Cornerstones of Information Warfare", Whitepaper, 1995.

[USC] U.S. Congress, Commission on the Roles and Capabilities of the United States Intelligence Community, *Preparing for the 21st Century: An Appraisal of U.S. Intelligence*, March 1, 1996.

[USCFR] Code of Federal Regulations, Title 47, Chapter 1

[USD(P)] Under Secretary of Defense for Policy, Infrastructure Policy Directorate, *Infrastructure Protection Briefing*, May, 1996.

[USGM] United States Government, *The United States Government Manual 1995/96*, Revised July 1, 1995.

[USNRC] U.S. Nuclear Regulatory Commission, Office of Nuclear Regulation, *The Price-Anderson System*, NOREG/BR-0079, Revision 1, Undated.

[USSPB] United States Security Policy Board, Personal Communications between Dan Knauf, Staff Member, and Bernard Ziegler, June 7, 1996.

[VIOLINO] Violino, Bob, "Crime Fighters," *Information Week*, May 13, 1996.

[WH 1] White House, Executive Order 12382, *National Security Telecommunications Advisory Committee*, September, 1982.

[WH 2] White House, Presidential Decision Directive 29, 1994.

[WH 3] White House, Presidential Decision Directive 39, 1995.

[YELTSIN] Yeltsin, Boris, *Action Program for 1996-2000*, Published under the headline "Russia: the individual, the family, the society, the state," BBC Summary of World Broadcasts Special Supplement, June 13, 1996.

This page intentionally left blank.

Acronyms

Acronyms

ACRONYMS

ACDA	Arms Control Disarmament Agency
ACS	Assistant Chief of Staff
ACSI	Assistant Chief of Staff for Intelligence
AFCSC	Air Force Cryptologic Support Center
AFIWC	Air Force Information Warfare Center
AFIWC	Air Force Information Warfare Center
AG	Attorney General
AGC	Automatic Generation Control
AIA	Air Intelligence Agency
AID	Agency for International Development
AMC	Advisory Management Committee
ARPA	Advanced Research Projects Agency
ASD(C3I)	Assistant Secretary of Defense for Command, Control, Communications and Intelligence
ASSIST	Automated Systems Security and Incident Support Team
AT&T	AT&T Corporation
ATIS	Alliance for Telecommunications Industry Solutions
ATM	Asynchronous Transfer Mode
ATM	Automated Teller Machine
BA	Bank of America
BAA	Broad Area Announcement
BELLCORE	Bell Communications Research, Incorporated
Boeing	The Boeing Company
C&D	Cover and Deception
C2	Command and Control
C2W	Command and Control Warfare
C3I	Command, Control, Communications, and Intelligence
C4I	Command, Control, Communications, Computers and Intelligence
CAC	Combined Arms Center
CASRIP	Center for Advanced Study and Research on Intellectual Property
CAT	Committee on Applications and Technology
CCEP	Commercial COMSEC Endorsement Program
CCI	Controlled Cryptographic Item
CCL	Commerce Control List
CD	Criminal Division
CD	Combat Developments
CDTD	Critical Defense Technology Division
CECOM	Communications-Electronics Command
CEI	Comparatively Efficient Interconnection
CERT	Computer Emergency Response Team
CFAA	Computer Fraud and Abuse Act
CFO	Chief Financial Officer

CFR	Code of Federal Regulations
CFTC	Commodities Futures Trading Corporation
CHIPS	Clearing House for Interbank Payments
CIA	Central Intelligence Agency
CIAC	Computer Incident Advisory Capability
CINC	Commander In Chief
CIO	Chief Information Officer
CISS	Center for Information Systems Security
CIWE	Center for Information Warfare Excellence
CJCS	Chairman, Joint Chiefs of Staff
CJCSI	Chairman, Joint Chiefs of Staff Instruction
CMC	Classification Management Committee
CMW	Compartmented Mode Workstation
CNA	Center for Naval Analyses
CNET	Chief, Naval Education and Training
CNO	Chief of Naval Operations
COAST	Computer Operation, Audit, and Security Technology
CoE	U.S. Army Corps of Engineers
COG	Continuity of Government
COMNAVSECGRU	Commander Naval Security Group
COMPUSEC	Computer Security
COMSAT	Communications Satellite Corporation
COMSEC	Communications Security
COP	Committee of Principals
CPAS	Cellular Priority Access Service
CPSR	Computer Professionals for Social Responsibility
CSAF	Chief of Staff Air Force
CSC	Computer Sciences Corporation
CSE	Center for Security Evaluations (DCI)
CSL	Computer Systems Laboratory
CSSPAB	Computer System Security and Privacy Advisory Board
CSTC	Computer Security Technology Center
CSTO	Computer Systems Technology Office
CT	Cryptologic Technician
CTSS	Computer and Telecommunications Staff
DAC/S	Deputy Assistant Chief of Staff
DARPA	Defense Advanced Research Projects Agency
DASD(C3)	Deputy Assistant Secretary of Defense (C3)
DCI	Director of Central Intelligence
DDCI	Deputy Director of Central Intelligence
DEA	Drug Enforcement Administration
DepAg	Deputy Attorney General
DepSecCommerce	Deputy Secretary of Commerce
DEPSECDEF	Deputy Secretary of Defense
DepSecNon-DefAg	Deputy Secretary of State, Non-Defense Agencies

DepSecState	Deputy Secretary of State
DES	Digital Encryption Standard
DHHS	Department of Health and Human Services
DIA	Defense Intelligence Agency
DII	Defense Information Infrastructure
DIRNSA	Director of National Security Agency
DISA	Defense Information Systems Agency
DISSP	Defense-Wide Information Systems Security Program
DIW	Defensive Information Warfare
DMRD	Defense Management Review Decision
DMS	Defense Message System
DoC	Department of Commerce
DoD	Department of Defense
DoDD	Deputy of Defense Directive
DoE	Department of Energy
DoEd	Department of Education
DoI	Department of the Interior
DoJ	Department of Justice
DOJIRS	DoJ Incident Response Service
DoS	Department of State
DoT	Department of Transportation
DoTreas	Department of Treasury
DP	Data Processor
DPA	Delegation of Procurement Authority
DPG	Defense Planning Guidance
DSB	Defense Science Board
DSS	Digital Signature Standard
DVA	Department of Veteran's Affairs
EAR	Export Administration Regulations
ECPMO	Electronic Commerce Program Management Office
EDS	Electronic Data Systems Corporation
EFF	Electronic Frontier Foundation
EIPC	Electronic Privacy Information Center
ELINT	Electronic Intelligence
EMP	Electromagnetic Pulse
EMS	Energy Management System
EO	Executive Order
EOP	Executive Office of the President
EPA	Environmental Protection Agency
ESC	Electronics Systems Center
ESNet	Energy Sciences Network
ESP	Enhanced Service Providers
et seq.	Et sequentes--and the following
EW	Electronic Warfare
FAA	Federal Aviation Administration

FACSPMF	Federal Agency Computer Security Program Manager's Forum
FAS	Foreign Agricultural Service
FAX	Facsimile Machine
FBI	Federal Bureau of Investigation
FCC	Federal Communications Commission
FDIC	Federal Deposit Insurance Corporation
FEDCAC	Federal Computer Acquisition Center
FEDSIM	Federal System Integration and Management
FEMA	Federal Emergency Management Agency
FERC	Federal Energy Regulatory Commission
FHA	Federal Highway Administration
FIPSPUBS	Federal Information Processing Standards Publications
FIRMRS	Federal Information Resources Management Regulations
FIRST	Forum of Incident Response and Security Teams
FISSP	Federal Information System Support Program
FIWC	Fleet Information Warfare Center
FNC	Federal Network Council
FPC	Facilities Protection Committee
FR	Federal Register
FRA	Federal Railroad Administration
FRS	Federal Reserve Service
FS	Forest Service
FTC	Federal Trade Commission
FTP	File Transfer Protocol
FTS2000	Federal Telecommunications System 2000
FY	Fiscal Year
GAO	General Accounting Office
GBS	Global Broadcast System
GETS	Government Emergency Telecommunications Service
GII	Global Information Infrastructure
GITS	Government Information Technology Service
GNSIE	Government Network Security Information Exchange
GPO	Government Printing Office
GPS	Global Positioning System
GSA	General Services Administration
GSII	Government Services Information Infrastructure
GSSP	Generally-accepted Systems Security Principles
GTE	GTE Corporation
HHS	Department of Health and Human Services
HPCC	High Performance Computing and Communications
HQMC	Headquarters, Marine Corps
HTCIA	High Technology Crime Investigative Association
HUMINT	Human Intelligence
I&W	Indications and Warning
I4	International Information Integrity Institute

IATF	Information Assurance Task Force
IBM	International Business Machines Corporation
ICC	Interstate Commerce Commission
ICCIP	Inter-Center Council on Information Processing
ICCITS	Inter-Center Council on Information Technology Security
ICCN	Inter-Center Council on Networking
IDA	Institute for Defense Analyses
IESG	Internet Engineering Steering Group
IETF	Internet Engineering Task Force
IIOO	INFOSEC Integration and Oversight Office
IITF	Information Infrastructure Task Force
IMPWG	Information Policy Working Group
IND	Industry
INFOSEC	Information Systems Security
INSCOM	Intelligence and Security Command
INTERPOL	International Criminal Police Organization
IO	Information Operations
IOSS	Interagency OPSEC Support Staff
IPC	Information Policy Committee
IPRWG	Intellectual Property Rights Working Group
IRM	Information Resources Management
IRMAC	Information Resource Management Advisory Committee
IRMC	Information Resources Management College
IRS	Internal Revenue Service
IRTF	Internet Research Task Force
IS	Intelligence Specialist
ISAT	Information Science and Technology
ISC	Information Systems Command
ISDN	Integrated Services Digital Network
ISMO	Information Security Management Office
ISOO	Information Security Oversight Office
ISSA	Information Systems Security Association
ISSAA	Information Systems and Software Acquisition Agency
ISSB	Information Systems Security Board
ISSC	Information Systems Security Committee
IT	Information Technology
ITA	Intermodel Transportation Agency
ITAR	International Traffic in Arms Regulation
ITMSC	Information Technology Management Council
ITS	Information Technology Service
ITSD	Information Technology Services Directorate
ITT	ITT Corporation
IW	Information Warfare
IW-D	Information Warfare - Defense
IWB	Information Warfare Branch

IWEB	Information Warfare Executive Board
JCADA	Supervisory Control and Data Acquisition
JCS	Joint Chiefs of Staff
JPSTC	Joint Program Office for Special Technical Countermeasures
JSC	Joint Security Commission
JTAV	Joint Total Asset Visibility
JWCA	Joint Warfighters Capability Assessment
KAPP	Key Asset Protection Program
KMI	Key Management Infrastructure
LAN	Local Area Network
LANL	Los Alamos National Laboratory
LANL	Los Alamos National Laboratory
LEAF	Law Enforcement Access Field
LIWA	Land Information Warfare Activity
LIWA	Land Information Warfare Activity
LLNL	Lawrence Livermore National Laboratory
Loral	Loral Corporation
MA	Maritime Administration
MARCO	Marine Corps
MCCDC	Marine Corps Combat Development Command
MCI	MCI Communications Corporation
MFS	MFS Communications Company, Incorporated
MI	Military Intelligence
MILSATCOM	Military Satellite Communications
MISSI	Multilevel Information Systems Security Initiative
MLS	Multilevel Security
MOE	Measure of Effectiveness
MOP	Memorandum of Policy
MOS	Military Occupational Specialty
MOU	Memorandum of Understanding
NACSEM	National Communications Security Emanations Memoranda
NACSI	National Communications Security Instruction
NACSIM	National Communications Security Information Memoranda
NADIR	Network Anomaly Detection Intrusion Reporter
NARA	National Archives and Records Administration
NAS	National Academy of Sciences
NASA	National Aeronautics and Space Administration
NATO	North Atlantic Treaty Organization
NCA	National Command Authority
NCC	National Coordinating Center
NCS	National Communications System
NCSC	National Computer Security Center
NDP	Navy Doctrine Publication
NDU	National Defense University
NEC	National Economic Council

NERC	North American Energy Reliability Council
NII	National Information Infrastructure
NIITF	National Information Infrastructure Task Force
NIST	National Institute of Standards and Technology
NIWA	Naval Information Warfare Activity
NRaD	Naval Research and Development Command
NRC	National Research Council
NRC	Nuclear Regulatory Commission
NRIC	Network Reliability and Interoperability Council
NRO	National Reconnaissance Office
NRSC	Network Reliability Steering Committee
NS/EP	National Security/Emergency Preparedness
NSA	National Security Agency
NSC	National Security Council
NSD	National Security Directive
NSDD	National Security Decision Directive
NSG	Naval Security Group
NSIE	Network Security Information Exchange
NSIERA	Network Security Information Exchange Risk Assessment
NSTAC	National Security Telecommunications Advisory Council
NSTC	National Science and Technology Council
NTI	Northern Telecom Incorporated
NTIA	National Telecommunications and Information Administration
NTISSC	National Telecommunications and Information Systems Security Committee
NTISSP	National Security Telecommunications and Information Systems Security Publication
NTMS	National Telecommunications Management Structure
NWC	Naval War College
OASA	Office of the Assistant Secretary of the Army
OASD(C3I)	Office of the Assistant Secretary of Defense for Command, Control, Communications and Intelligence
OASIS	Open Access Same Time Information System
OCC	Office of the Comptroller of the Currency
ODCSINT	Office of the Deputy Chief of Staff for Intelligence
ODCSOPS	Office of the Deputy Chief of Staff for Operations and Plans
ODISC4	Office of the Director of InformationSystems for C4
OECD	Organization for Economic Cooperation and Development
OIS	Office of Information Security
OIW	Offensive Information Warfare
OMB	Office of Management and Budget
OMNCS	Office of the Manager, National Communications System
ONA	Open Network Architecture
ONA	Office of Net Assessment
OPM	Office of Personnel Management

OPNAV	Office of the Chief of Naval Operations
OPNAVINST	Office of the CNO Instruction
OPSEC	Operations Security
OS	Operations Specialist
OSD	Office of the Secretary of Defense
OSI	Office of Special Investigations
OSTP	Office of Science and Technology Policy
OSWR	Office of Science and Weapons Research
OTA	Office of Technology Assessment
OTCIXS	Office-in-Tactical Command Information Exchange Subsystem
OTS	Office of Thrift Supervision
OWTP	Office of Weaponry Technology and Proliferation
PCAST	President's Committee of Advisors on Science and Technology
PCERT	Pursue Computer Emergency Response Team
PDD	Presidential Decision Directive
PEM	Privacy Enhanced Mail
PGP	Pretty Good Privacy
PIC	Policy Integration Committee
PIN	Personal Identification Number
PKCS	Public Key Cryptography Standards
PLC	Power-line Carrier
PM	Program Manager
PNNL	Pacific Northwest National Laboratory
POC	Point of Contact
POM	Program Objective Memorandum
PRD	Presidential Review Decision
PSC	Personnel Security Committee
PSN	Public Switched Network
PSYOP	Psychological Operations
PTI	Pacific Telecom, Incorporated
R&D	Research and Development
RBOC	Regional Bell Operating Company
RDA	Research, Development, and Acquisition
RM	Radioman
RSA	Rivert, Shamir, Adleman
RVWG	Reliability and Vulnerability Working Group
S&T	Science and Technology
SARDA	(Assistant) Secretary of the Army for Research, Development, and Acquisition
SATAN	Security Administrator's Tool for Analyzing Networks
SC	Assistant Chief of Staff for C4 (Office Code)
SEALS	Sea Air Land (Special Operations)
SEC	Securities and Exchange Commission
SECDEF	Secretary of Defense
SIF	Security Issues Forum

SIGINT	Signals Intelligence
SISS	Subcommittee on Information Systems Security
SIWS	School of Information Warfare and Strategy
SNL	Sandia National Laboratory
SOCS	Subcommittee on Computer Security
SONET	Synchronous Optical Network
SOP	Standard Operating Procedure
SPB	U.S. Security Policy Board
SSA	Social Security Administration
STS	Subcommittee on Telecommunications Security
TIIAP	Telecommunications and Information Infrastructure Assistance Program
TIS	Trusted Information Systems, Inc.
TPC	Telecommunications Policy Committee
TPDC	Training and Professional Development Committee
TRADOC	US Army Training and Doctrine Command
TRANSCOM	U.S. Transportation Command
TRW	TRW Incorporated
TSP	Telecommunications Service Priority System
U.S.	United States
U.S. West	U.S. West Incorporated
UCC	Uniform Commercial Code
UNISYS	UNISYS Corporation
UnSecEnergy	Under Secretary of Energy
US(E)	Under Secretary for Enforcement
USA	United States Army
USAC	U.S. Advisory Council
USAF	United States Air Force
USCG	United States Coast Guard
USD(A&T)	Undersecretary of Defense for Acquisition and Technology
USD(P)	Undersecretary of Defense for Policy
USDA	U.S. Department of Agriculture
USIA	United States Information Agency
USMC	United States Marine Corps
USN	United States Navy
USNPGS	U.S. Naval Post-Graduate School
USPS	United States Postal Service
USSS	United States Secret Service
USTA	United States Telephone Association
VCJCS	Vice Chairman, Joint Chiefs of Staff
VTC	Video Teleconference
WAN	Wide Area Network
WG	Working Group
WGET	Working Group on Encryption and Telecommunications
WILTEL	Williams Telecommunications Group Incorporated

XIWT	Cross Industry Working Team
XO	Deputy Chief of Staff for Operations (Office Code)
XOX	Assistant Deputy Chief of Staff for Operations (Office Code)

Glossary

Glossary

GLOSSARY

NOTE: The source of a definition is shown in brackets, when available. Multiple definitions and their sources are shown where there is significant variance between definitions.

Access Control -- A means of preventing the unauthorized use of a resource or the use of a resource in an unauthorized manner.

Accountability -- The property that enables activities on an automated information system to be traced to individuals who may then be held responsible for their actions.

Assurance -- A measure of confidence that the security features and architecture of an AIS accurately mediate and enforce the security policy. If the security features of an AIS are relied on to protect classified or sensitive unclassified information and restrict user access, the features must be tested to ensure that the security policy is enforced and may not be circumvented during AIS operation. [DODD 5200.28, 1988]

Attack Assessment -- An evaluation of information to determine the potential or actual nature and objectives of an attack for the purpose of providing information for timely decisions. [CJCS Joint Pub 1-02, Mar 94]

Authenticate -- To establish the validity of a claimed identity.

Availabilty -- Ensuring that data transmission or computing processing systems are not denied to authorized users. [CJCSI 6510.01A, 1996]

Availability of Services -- An assured level of service, capacity, quality, timeliness, and reliability.

Classified National Security Information -- Information that has been determined pursuant to Executive Order 12958 or any predecessor order to require protection against unauthorized disclosure and is marked to indicate its classified status when in documentary form. [Executive Order 12958, Apr. 95]

Command and Control Warfare (C2W) -- The integrated use of operations security (OPSEC), military deception, psychological operations (PSYOP), electronic warfare (EW) and physical destruction, mutually supported by intelligence, to deny information to, influence, degrade or destroy adversary C2 capabilities, while protecting friendly C2 capabilities against such actions. Command and Control Warfare applies across the operational continuum and all levels of conflict. Also called C2W. C2W is both offensive and defensive: a. Counter-C2-- to prevent effective C2 of adversary forces by denying information to, influencing, degrading, or destroying the adversary C2 system. b. C2-Protection -- To maintain effective command and control of own forces by turning to friendly advantage or negating adversary efforts to deny information to, influencing, degrade, or destroy the friendly C2 system. [CJCS MOP 30, 1993, *Joint Pub 1-02, 1994*] *NOTE: In Joint Pub 1-02, 1994, this definition of C2W is a replacement for Command, Control, and Communications Countermeasures.*

Commercial-off-the-shelf (COTS) -- Commercial items that require no unique Government modifications or maintenance over the life cycle of the product to meet the needs of the procuring agency.

Communications Security (COMSEC) -- Measures and controls taken to deny unauthorized persons information derived from telecommunications and ensure the authenticity of such telecommunications. Communications security includes cryptosecurity, transmission security, and physical security of COMSEC material. [NSTISSI 4009, 1992]

Continuity of Operations -- The degree or state of being continuous in the conduct of functions, tasks, or duties necessary to accomplish a military action or mission in carrying out the national military strategy. It includes the functions and duties of the commander, as well as the supporting functions and duties performed by the staff and others acting under the authority and direction of the commander. [Joint Pub 1.02]

Critical Infrastructures -- Infrastructures that are deemed to be so vital that their incapacity or destruction would have a debilitating regional or national impact. They include at least seven categories: telecommunications; electrical power systems; gas and oil; banking and finance; transportation; water supply systems; continuity of government and government operations. Emergency services (including medical, police, and fire and rescue services) might also be considered critical infrastructures.

Damage Assessment -- 1. The determination of the effect of attacks on targets. (DoD) 2. A determination of the effect of a compromise of classified information on national security. [CJCS Joint Pub 1-02, Mar 94]

Damage to the National Security -- Harm to the national defense or foreign relations of the United States from the unauthorized disclosure of information, to include the sensitivity, value, and utility of that information. [Executive Order 12958, Apr. 95]

Data -- Representation of facts, concepts, or instructions in a formalized manner suitable for communications, interpretation, or processing by humans by automatic means. Any representations such as characters or analog quantities to which meaning is, or might be, assigned.

Defense Information Infrastructure (DII) -- The DII encompasses information transfer and processing resources, including information and data storage, manipulation, retrieval, and display. More specifically, the DII is the shared or interconnected system of computers, communications, data, applications, security, people, training, and other support structure, serving the DoD's local and worldwide information needs. The DII (1) connects DoD mission support, command and control, and intelligence computers and users through voice, data, imagery, video, and multimedia services, and (2) provides information processing and value-added services to subscribers over the DISN. Unique user data, information, and user applications are not considered part of the DII. [ASD(C3I) Memo, 1994]

Defense Information Systems Network (DISN) -- 1. A subelement of the DII, the DISN is the DoD's consolidated worldwide enterprise level telecommunications infrastructure that provides the end-to-end information transfer network for supporting military operations. It is transparent to its users, facilitates the management of information resources, and is responsive to national security and defense needs under all conditions in the most efficient manner. [ASD(C3I) Memo, 1994] 2. The DISN is an information transfer network with value-added services for supporting national defense C3I decision support requirements and CIM functional business areas. As a information transfer utility, the DISN provides dedicated point-to-point, switched voice and data, imagery and video teleconferencing communications services. [CJCSI 6211.02, 1993]

Defensive Counterinformation -- Actions protecting our military information functions from the adversary. [Air Force Cornerstones of Information Warfare, released in Aug. 95]

Defensive Information Warfare (IW-D) -- IW-D is process that integrates and coordinates policies and procedures, operations, intelligence, law, and technology to protect information and defend information systems. The objective of IW-D is to ensure access to timely, accurate, and relevant information when and where it is needed and to deny an adversary the opportunity to exploit friendly information and systems for their own purposes. Effective IW-D implementaiton ensures the availability, integrity, authentication, confidentiality, and non-repudiation of US Government information and required service levels of US Government information systems. [CJCSI 6510.01A, 1996]

Denial of Service -- Action or actions that result in the inability of an AIS or any essential part to perform its designated mission, either by loss or degradation of operational capability. [DODD 5200.28, 1988]

Disruption -- 1. Denial of service or corruption of information resulting from a single event, cause, or source; whether direct or indirect, accidental or intentional, rare or common. 2. Uncertainty - denial of services, information corruption.

Electronic Warfare (EW) -- 1. Any military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy. Also called EW. The three major subdivisions within electronic warfare are: electronic attack, electronic protection, and electronic warfare support. [Joint Pub 1-02, 1994] 2. Military action involving: (1) the use of electromagnetic or directed energy to attack an enemy's combat capability, (2) protection of friendly combat capability against undesirable effects of friendly or enemy employment of electronic warfare or, (3) surveillance of the electromagnetic spectrum for immediate threat recognition in support of electronic warfare operations and other tactical actions such as threat avoidance, targeting, and homing. Also called EW. [CJCS MOP 6, 1990]

Function -- Appropriate or assigned duty, responsibility, mission, task, power, or duty of an individual, office, or organization. A functional area (e.g., Personnel) comprises of one or more functional activities (e.g., recruiting), each of which consists of one or more functional processes (e.g., interviews).

Global Information Infrastructure (GII) -- Includes the information systems of all countries, international and multinational organizations and multi-international commercial communications services.

Government Services Information Infrastructure (GSII) -- The U.S. Government information infrastructure. A subset of the NII. Sometimes referred to as Government Information Technology Services (GITS).

Hacker -- 1. A person who enjoys exploring the details of programmable systems and how to stretch their capabilities, as opposed to most users, who prefer to learn only the minimum necessary [The New Hackers Dictionary, on-line]; 2. Unauthorized user who attempts or gains access to an information system. [NSTISSI No. 4009, January 1996]

Heterogeneous Networks -- Networks composed of hardware and software supplied by multiple vendors usually implementing multiple protocols.

Identification and Authentication -- Verification of the originator of a transaction, similar to the signature on a check or a Personal Identification Number (PIN) on a bank card. [CJCSI 6510.01A, 1996]

Imagery -- Collectively, the representation of objects reproduced electronically or by optical means on file, electronic display devices, or other media.

Indications and Warning -- Those are intelligence activities intended to detect and report time-sensitive intelligence information on foreign developments that could involve a threat to the United States or allied military, political, or economic interests or to US citizens abroad. It includes forewarning of enemy actions or intentions; the imminence of hostilities; insurgency; nuclear/non-nuclear attack on the United States, its overseas forces, or allied nations; hostile reactions to United States reconnaissance activities; terrorist attacks; and other similar events. [CJCS Joint Pub 1-02, Mar 94]

Information -- Knowledge such as facts, data, or opinions, including numerical, graphic, or narrative forms, whether oral or maintained in any medium.

Information Assurance -- The availability of services and information integrity.

Information Integrity -- The state that exists when information is unchanged from its source and has not been accidentally or intentionally modified, altered, or destroyed. [Executive Order 12958, Apr. 95]

Information Security -- The Protection of information against unauthorized disclosure, transfer, modification, or destruction, whether accidental or intentional. [FED-STD-1037B, 1991]

Information Superiority -- That degree of dominance in the information domain which permits the conduct of operations without effective opposition. (Unclassified) [DoDD S-3600.1 (Draft), 1995]

Information System -- The organized collection, processing, transmission, and dissemination of information in accordance with defined procedures, whether automated or manual. In information warfare, this includes the entire infrastructure, organizations, and components that collect, process, store, transmit, display, and disseminate information. [DoDD S-3600.1 (Draft, 1995)]

Information Systems Security -- 1. The protection of information systems against unauthorized access to or modification of information, whether in storage, processing, or transit, and against denial of service to authorized users or the provision of service to unauthorized users, including those measures necessary to detect, document, and counter such threats. [NSTISSI 4009, 1992] 2. A composite of the means of protecting telecommunications systems and automated information systems and the information they process. [FED-STD 1037B, 1991]

Information Warfare (IW) -- Actions taken to achieve information superiority by affecting adversary information, information-based processes, information systems, and computer-based networks while defending one's own information, information-based processes, information systems, and computer-based networks. [CJCSI 3210.01, 1996]

Infrastructure -- The framework of interdependent networks and systems comprising identifiable industries, institutions, and distribution capabilities that provide a continual flow of goods and services essential to the defense and economic security of the United States, to the smooth functioning of governments at all levels, and to society as a whole. [CIWG]

Infrastructure Assurance -- The surety of readiness, reliability, and continuity of infrastructures such that they are: (1) less vulnerable to disruptions or attack; (2) harmed to a lesser degree in the event of a disruption or attack; and (3) can be readily reconstituted to reestablish vital capabilities. [CIWG]

Integrated Network Management -- Network Management is the set of activities to provide and establish networking and information processing resources, keep them operational, fine tune their operation, account for their usage, and support their protection from unauthorized use and tampering. Typically, the term also refers to these management activities as well as a myriad of other management functions and activities, of greater or lesser scope, when any of these management functions and activities are applied. Other management functions and activities may be associated with utilization. Other resources may include general purpose information processing resources such as computers, their system software and/or peripherals, the distributed multimedia applications they host, or the aggregate of all such resources together with the networking resources used to interconnect them.

Integrity -- Absolute verificaiton that data has not been modified in transmission or during computer processing. [CJCSI 6510.01A, 1996]

Intelligence Estimate -- The appraisal, expressed in writing or orally, of available intelligence relating to a specific situation or condition with a view to determining the courses of action open to the enemy or potential enemy and the order of probability of their adoption. [CJCS Joint Pub 1-02, Mar 94]

Interoperability -- The ability of two or more systems or components to exchange and use information.

Legacy -- Existing.

Local Area Network (LAN) -- A data network, located on a user's premises, within a limited geographic region. Communication within a local area network are not subject to external regulation; however, communications across the network boundary may be subject to some form of regulation.

National Information Infrastructure (NII) -- The NII is a system of high-speed telecommunications networks, databases, and advanced computer systems that will make electronic information widely available and accessible. The NII is being designed, built, owned, operated, and used by the private sector. In addition, the government is a significant user of the NII. The NII includes the Internet, the public switched network, and cable, wireless, and satellite communications. It includes public and private networks. As these networks become more interconnected, individuals, organizations, and governments will use the NII to engage in multimedia communications, buy and sell goods electronically, share information holdings, and receive government services and benefits. [NII Security: The Federal Role, 1995]

National Security Systems -- Those telecommunications and information systems operated by the US Government, its contractors, or agents, that contain classified information or, as set forth in 10 USC Section 2315, that involve intelligence activities, involve cryptologic activities related to national security, involve command and control of military forces, involve equipment that is an integral part of a weapon or weapon system, or involve equipment that is critical to the direct fulfillment of military or intelligence missions. [NSD-42, 1990]

Nonrepudiation -- The ability to prove the identity of the sender and receiver of an electronic transmission, as well as to verify the transmission and receipt of the message, so that the parties cannot claim not to have sent or received the transmission. Digital signatures are the current non-repudiation technique of choice for the NII.

Open Network Architecture -- A regulatory framework imposed by the FCC on communications carriers (the long distance telephone carriers such as AT&T and the Regional Bell Operating Companies) which requires the carriers to provide competing service providers with access to basic communications services on an equal basis. [NIST Special Pub 800-11, Feb. 95]

Open System -- A system that implements sufficient open specifications for interfaces, services, and supporting formats to enable properly engineered applications software: (a) to be ported with minimal changes across a wide range of systems, (b) to interoperate with other applications on local and remote systems, and (c) to interact with users in a style that facilitates user portability.

Open Systems Environment (OSE) -- The comprehensive set of interfaces, services, and supporting formats, plus user aspects for interoperability or for portability of applications, data, or people, as specified by information technology standards and profiles.

Open Systems Interconnection (OSI) Reference Model -- The adopted architectural model for network services in the DoD technical Architecture Framework developed for standardizing communications interfaces and protocols.

Operations Security (OPSEC) -- OPSEC is a process of identifying critical information and subsequently analyzing friendly actions attendant to military operations and other activities to: Identify those actions that can be observed by adversary intelligence systems; Determine indicators adversary intelligence systems might obtain that could be interpreted or pieced together to derive critical information in time to be useful to adversaries; Select and execute measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation. [Joint Pub 3-54, 1991]

Personal Communications Services (PCS) -- Personal Communications Services is a set of capabilities that allows some combination of terminal mobility, personal mobility, and service profile management.

Precedence -- A rank ordering assigned to indicate the degree of preference given in processing and protecting communications traffic.

Protocol -- A collection of rules, voluntarily agreed upon by vendors and users to ensure that equipment transmitting and receiving data understand each other. Protocols comprise three major areas: the method in which data is represented or coded; the method in which codes are received; and the methods used to establish control, detect failures or errors, and initiate corrective action.

Psychological Operations (PSYOP) -- PSYOP are operations planned to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning and, ultimately, the behavior of foreign governments, organizations, groups, and individuals. The purpose of PSYOP is to induce or reinforce foreign attitudes and behavior favorable to the originator's objectives. PSYOP are a vital part of the broad range of US political, military, economic, and informational activities. When properly employed, PSYOP can lower the morale and reduce the efficiency of enemy forces and could create dissidence and disaffection within their ranks. [Joint Pub 3-53, 1993]

Risk -- The probability that a particular threat will exploit a particular vulnerability of the system. [NSA, NCSC Glossary, Oct. 88]

Risk Analysis -- The process of identifying security risks, determining their magnitudes, and identifying areas needing safeguards. Risk analysis is a part of risk management. Synonymous with risk assessment. [NSA, NCSC Glossary, Oct. 88]

Risk Assessment -- Synonymous with risk analysis. [NSA, NCSC Glossary, Oct. 88]

Risk Management -- The total process of identifying, controlling, and eliminating or minimizing uncertain events that may affect system resources. It includes risk analysis, cost benefit analysis, selection, implementation and test, security evaluation of safeguards, and overall security review. [NSA, NCSC Glossary, Oct. 88]

Security Management -- Security Management is one of the five major SMFAs described in the ISO Management Framework and System Management Overview standards. Security Management includes those actions taken to support combat of threats by identifying and logging users of sensitive resources, monitoring usage of sensitive resources, defining, identifying, and monitoring security-relevant events, creating, and analyzing audit trails of such events, users and usage, controlling certain aspects of security services and mechanisms, and controlling configuration.

Sensitive Information -- Information, the loss, misuse, or unauthorized access to modification of which could adversely affect the national interest or the conduct of federal programs, or the privacy to which individuals are entitled under 5 U.S.C. Section 552a (the Privacy Act), but that has not been specifically authorized under criteria established by an Executive Order or and Act of Congress to be kept secret in the interest of the national defense or foreign policy. (Systems that are not national security systems, but contain sensitive information are to be protected in accordance with the requirements of the Computer Security Act of 1987 (P.L. 100-235).) [NSTISSI No. 4009, January 1996]

Social engineering -- Deceiving human operators of information systems into revealing privileged information such as modem dial-in numbers and account passwords

Stovepiped Systems -- Vertically integrated systems that perform the whole range of functions required for a particular application.

Tactical Warning -- 1. A warning after initiation of a threatening or hostile act based on an evaluation of information from all available sources. 2. In satellite and missile surveillance, a notification to operational command centers that a specific threat event is occurring. The component elements that describe threat events are: Country of origin--country or countries initiating hostilities. Event type and size--identification of the type of event and determination of the size and number of weapons. Country under attack--determined by observing trajectory of an object and predicting impact point. Event time--time the hostile event occurred. [CJCS Joint Pub 1-02, Mar 94]

Technical Attack -- Attack that can be perpetrated by circumventing or nullifying hardware or software protection mechanisms, rather than by subverting system personnel or other users. [NSTISSI 4009, 1992]

Transmission Security (TRANSEC) -- Component of communications security that results from the application of measures designed to protect transmissions from interception and exploitation by means other than cryptoanalysis. [NSTISSI 4009, 1992]

Trashing -- Hacker term for physically searching garbage for useful information about the target site such as manuals, telephone numbers, passwords, proprietary information, internal memos, etc.

Utility -- An element of the DII providing information services to DoD users. These services include DISA [DoD] Megacenters, information processing, and wide area network communications devices. [ASD(C3I) Memo, 1994]

This page intentionally left blank.

Index

Index

This page intentionally left blank.